Nadzor nad obavještajnim službama

Priručnik

Urednici: Hans Born i Aidan Wills

DCAF
a centre for security, development and the rule of law

Ministry of Foreign Affairs of the Netherlands

Nadzor nad obavještajnim službama

Priručnik

Urednici: Hans Born i Aidan Wills

DCAF
a centre for security, development and the rule of law

Ministry of Foreign Affairs of the Netherlands

Ženevski centar za demokratsku kontrolu nad oružanim snagama (DCAF) je međunarodna fondacija čija je misija pomoći međunarodnoj zajednici u težnji za dobrim upravljanjem i reformom sigurnosnog sektora. Centar razvija i promovira norme i standarde, provodi specifična istraživanja na planu politika, identificira dobre prakse i preporuke radi promocije demokratskog upravljanja sigurnosnim sektorom, te pruža savjetodavnu podršku i programe praktične pomoći na licu mjesta u samim zemljama.

Izdavač: DCAF, Ženeva
11 Rue de Chantepoulet
Geneva – 1201
Switzerland
www.dcaf.ch

Dizajn: Alice Lake-Hammond, www.alicelakehammond.com
Redaktura: Agincourt Press
Prijevod: Senada Kreso
Recenzija prijevoda: Predrag Petrović
Fotografija na koricama: Hans Kouwenhoven

Ova publikacija je omogućena zahvaljujući velikodušnoj podršci Ministarstva vanjskih poslova Holandije.

Napomena izdavača:
Mišljenja iznesena u ovom priručniku su mišljenja autora pojedinačnih tekstova i ne održavaju obavezno mišljenja urednika, ni institucionalne pozicije DCAF-a, niti Ministarstva vanjskih poslova Holandije. Ni DCAF, ni Ministarstvo vanjskih poslova Holandije ne snose odgovornost za iskazana gledišta, niti za tačnost činjenica i drugih oblika informacija sadržanih u ovoj publikaciji.

ISBN: 978-92-9222-225-3

Sadržaj

Spisak tabela i okvira

DCAF-ov predgovor

Obavještajni sektor predstavlja krajnju granicu u procesima demokratizacije i reforme sigurnosnog sektora. Kao što su pokazale mnoge etablirane demokratije, demokratsko upravljanje i vladavina prava bivaju uspostavljeni u obavještajnom sektoru dugo nakon što su dobro etablirani u drugim područjima djelovanja države. U mnogim etabliranim demokratijama, izgradnja sistema obavještajnog nadzora prati uobičajenu putanju: određene aktivnosti obavještajnih i sigurnosnih službi izazivaju zabrinutost zbog ugrožavanja legitimnih demokratskih procesa i ostvarenja prava i temeljnih sloboda, što je dovodilo do istraga i postavljanja pitanja, te su kao rezultat toga uspostavljeni novi nadzorni mehanizmi.

Demokratije u nastajanju ne treba da koristite ovaj reaktivni pristup. „Tranzicija“ im pruža zlatnu priliku da polože snažni zakonski i institucionalni temelj za nadzor nad obavještajnim službama. Međutim, ovde moramo biti oprezni budući da je polaganje tih temelja tek mali korak u neprekidnom i izazovnom procesu osiguravanja da obavještajne službe nisu samo učinkovite u pogledu zaštite nacionalne sigurnosti, javne sigurnosti i ljudskih prava, već da također poštuju vladavinu zakona i demokratsku praksu. Dugoročno postizanje ovih ciljeva zahtijeva od aktera uključenih u nadzor stalnu zainteresiranost, budnost i predanost ovom poslu, kao i ustrajno nastojanje da se sistemi nadzora ocjenjuju i unapređuju. Uvjeren sam da ovaj priručnik može služiti kao važan resurs podrške u tome poslu.

Parlamentarci snose veliku odgovornost, kako za razvoj pravnog i institucionalnog okvira za nadzor, tako - kao glavni vanjski akteri nadzora - i za osiguravanje da nadzor postigne navedene ciljeve. Na tom polju, više nego na bilo kojem drugom, parlamentarci se moraju boriti da svoje partijske i političke interese podrede višem cilju zaštite demokratskog i ustavnog poretka. Naravno, parlamentarce same ne treba preopteretiti svim odgovornostima koje sobom nosi vanjski nadzor, jer oni često nemaju ni vremena, ni stručnog znanja, a ni potrebnu nezavisnost za to. S obzirom na to, oni moraju tražiti da nezavisna zakonska nadzorna tijela, kao što su glavne revizorske institucije, institucije ombudsmena i stručna nadzorna tijela, igraju ključnu ulogu – svako u svom području nadležnosti.

I pored toga što postoji veliki broj publikacija koje se bave nadzorom nad obavještajnim službama, većina ih je usmjerena samo na pravne i institucionalne okvire za nadzorna tijela. Ovaj priručnik oslanja se na taj pristup time što donosioce odluka vodi kroz brojne

izazove i probleme koje se javljaju u kreiranju, dopuni i konsolidaciji sistema nadzora. Ipak, autori ovog priručnika usudili su se da idu dalje, ponudivši jasne praktične smjernice o tome kako da se vanjska nadzorna tijela nose sa izazovima kontrole specifičnih područja rada obavještajnih i sigurnosnih službi. Nadam se da ovaj priručnik može poslužiti i za podizanje svijesti u civilnom društvu i medijima o značaju različitih aspekata nadzora nad obavještajnim službama, te da će te grupe moći koristiti ove spoznaje kako bi parlamentarce i druga nezavisna nadzorna tijela učinili odgovornim za svoju obavezu kontrole (ili njenog nepostojanja) obavještajnih službi.

Ovaj priručnik će po svoj prilici biti najzanimljiviji donosiocima odluka, uključenim u razvijanje sistema nadzora nad obavještajnim službama, članovima i službenicima novouspostavljenih nadzornih tijela, kao i organizacijama civilnog društva. Dok je većina njih vjerovatno u zemljama u tranziciji, ne treba zanemariti ni vrijednost saznanja autora ovog priručnika za one koji su uključeni – bilo direktno ili indirektno – u nadzor nad obavještajnim službama u etabliranim demokratijama. Doista, ja čvrsto vjerujem da ovaj priručnik nudi primjere i argumente koji će izazvati diskusije o mogućim proširenjima ili jačanjima politika nadzora u tim političkim sistemima.

Više od deset godina DCAF pruža podršku nastojanjima na jačanju kapaciteta nadzora nad obavještajnim službama, ne samo u demokratijama u nastanku, već i u mnogo etabliranijim demokratskim sistemima. DCAF smatra da je reforma sistema nadzora nad obavještajnim službama sastavni dio procesa reformi sigurnosnog sektora u kontekstu tranzicije. Dok pojedini donatori posvećuju značajan dio resursa jačanju operativnog kapaciteta obavještajnih službi u zemljama u tranziciji (kako bi u njima dobili učinkovite operativne partnere), od izuzetnog je značaja da i države donatori i države primaoci donacija ulažu u razvoj i održavanje trajnih i učinkovitih sistema nadzora. Nadam se da ovaj priručnik može doprinijeti uspostavljanju ravnoteže između operativne učinkovitosti i demokratskog upravljanja, podizanjem svijesti o neophodnosti nadzora nad obavještajnim službama u zajednici koja se bavi reformom sigurnosnog sektora.

Ambasador Theodor H. Winkler
Direktor, DCAF

Predgovor

Kao dijete, bio sam fasciniran kaleidoskopima a to sam i sad kao odrastao čovjek. Sve što u rukama imate je samo malena cijev sa poklopcem od mliječnog stakla na jednoj strani, i okruglom rupicom, na drugoj. Protresete li pažljivo tu cijev, obično se čuje blago zveckanje. Ali nemate pojma šta je u njoj.

Kada pogledate kroz rupicu ništa ne vidite, osim ako ne držite cijev tako da svjetlo pada na njeno mliječno staklo. Tek tad iznenada vidite kompleksan mozaik. A kada okrenete cijev naopačke, vidite kako se mijenja šara mozaika – što je fascinantno.

Na izvjestan način, ova knjiga je nalik na kaleidoskop. Na kraju krajeva, obavještajni rad jeste crna kutija s kojom se mora rukovati na određen način da bi se stekao uvid u nju. Štaviše, čini se da se perspektiva neprekidno mijenja.

Ono što pažljiviji posmatrač vidi ipak je uvijek vrijedno pažnje, i zanimljivo je onoliko koliko je posmatrač voljan podijeliti to što vidi sa drugima. To, zapravo, nije tako jednostavno kao što se čini stoga što se tajne cjevčice u kojoj je sadržan obavještajni svijet jednostavno ne mogu tek tako otkriti.

Namjera ove knjige je da na strukturiran način ponudi instrumente koje omogućavaju nadzornim tijelima da na pravi način okrenu cijev prema svjetlu te da potom na utemeljen način druge izvijeste o onome što su zapazila.

Opisujući ove instrumente, autori su osvijetlili razne aspekta nadzora, postavljajući razne sisteme nadzora jedan uz drugog, stvarajući tako kaleidoskopsku sliku koja jasno svjedoči o činjenici da postoji više od jednog tipa nadzora, te nas poziva da kontinuirano posmatramo čudesni svijet obavještajnog rada iz svježeg i kritičkog ugla gledanja.

Koristi od ove knjige će imati ne samo oni koji su izvan svijeta ovih službi a zainteresirani su za ovu temu, veći zasigurno i oni koji su unutar ovog svijeta, tzv. insajderi – nadzorna tijela i oni koji su predmet nadzora.

Bert van Delden
Predsjednik Odbora za nadzor obavještajnih i sigurnosnih službi Kraljevine Holandije

Reči zahvalnosti

Urednici žele izraziti zahvalnost Ministarstvu vanjskih poslova Holandije, čija je velikodušna finansijska podrška omogućila izradu ovog priručnika. Posebno želimo zahvaliti sljedećim članovima Odjela za sigurnosno-odbrambenu politiku na njihovoj dragocjenoj podršci i saradnji, pruženoj neprekidno tokom izrade ovog priručnika: Jaccou Bosu, Heinu Knegtu, Michaelu Stibbeu, Franku van Beuningenu i Joepu Wijnandsu.

Želimo također zahvaliti za doprinos holandskom Odboru za ocjenu obavještajnih i sigurnosnih službi (CTIVD), a posebno njegovom predsjedniku, Bertu van Deldenu; bivšem sekretaru, Nicku Verhoevenu, kao i sadašnjem sekretaru Odbora, Hilde Bos-Ollerman. CTIVD je pružio bitnu podršku prilikom pokretanja ovog projekta, te je velikodušno ponudio svoje stručno znanje tokom izrade priručnika. Urednici žele također iskazati zahvalnost bivšem holandskom ministru odbrane i senatoru Wimu van Eekelenu, čija je podrška DCAF-u bitna za uspjeh ovog projekta.

Nadalje, urednici osjećaju dug prema Agincourt Press, čiji uposlenici su odgovorni za korekturu i lekturu najvećeg dijela ove knjige. Uposlenici Agincourt Press-a su neumorno radili kako bi osigurali konzistentnost jezika i stila, te da ovaj priručnik bude, koliko god je to moguće, dostupan publici koja nije stručna. Također želimo zahvaliti Alice Lake-Hammond na izvrsnom radu na dizajniranju, te na njenom visoko profesionalnom pristupu u tehničkoj pripremi teksta za štampu.

Konačno, želimo zahvaliti našem bivšem kolegi, Gabrielu Geisler Mesevageu, koji ne samo da je koautor uvodnog teksta, već je dao i značajan doprinos konceptualizaciji i izradi ovog priručnika.

Hans Born i Aidan Wills
Ženeva, juli 2012.

POGLAVLJE 1

Uvod u nadzor nad obavještajnim službama

Hans Born i Gabriel Geisler Mesevage

1

Uvod u nadzor nad obavještajnim službama

Hans Born i Gabriel Geisler Mesevage

1. UVOD

Ovo poglavlje uvodi čitaoca u temu nadzora nad obavještajnim službama, pri čemu daje koncizne odgovore na osnovna pitanja o tome ko, šta, kada, kako i zašto nadzire obavještajne službe. On, također, uvodi čitaoce u druga poglavlja u ovom priručniku o nadzoru nad obavještajnim službama, koje, zajedno, pružaju detaljnije odgovore na ta, kao i na neka druga pitanja.

Cilj ovog projekta je objediniti neke od najistaknutijih svjetskih stručnjaka na polju nadzora nad obavještajnim službama kako bi izložili svoje stručno znanje na način koji je razumljiv i onima koji nisu stručni u ovoj oblasti. Ovaj priručnik je posebno zamišljen da pomogne čitaocima da bolje razumiju bitna pitanja te da ona koja su vezana za nadzor sagledaju kroz cijeli niz komparativnih perspektiva.

Uvodno poglavlje počinje pregledom procesa nadzora nad obavještajnim službama, uključujući opis institucija koje su u to uključene te „ciklus nadzora nad obavještajnim službama“. Potom objašnjava zašto je nadzor nad obavještajnim službama važan za zaštitu ljudskih prava i temeljnih sloboda pojedinaca, kao i za njihovu veću sigurnost. Poglavlje, nadalje, daje pregled aktuelnih standarda i praksi na polju nadzora nad obavještajnim službama, fokusirajući se na ono što većina stručnjaka smatra dobrim praksama. U zaključku su date preporuke za jačanje nadzora nad obavještajnim službama.

1.1 ZAŠTO NUDIMO OVAJ PRIRUČNIK ZA NADZOR NAD OBAVJEŠTAJNIM SLUŽBAMA?

Ovaj priručnik je sačinjen kako bi pomogao novim demokratijama da uspostave — a etabliranim demokratijama da poboljšaju — civilni nadzor nad obavještajnim službama. On ima četiri glavna cilja:

1. pružiti smjernice relevantne za politike stvaranja i konsolidacije novih sistema nadzora, kao i za razmatranje i poboljšanje postojećih sistema;
2. pružiti smjernice o nadzoru posebnih područja aktivnosti obavještajnih službi, uključujući prikupljanje informacija, korištenje ličnih podataka i razmjenu informacija;
3. podići svijest o značaju nadzora nad obavještajnim službama među pripadnicima civilnog društva i u medijima;
4. promovirati učenje u cijeloj zemlji, te prenošenje normi kroz identifikaciju i analizu različitih pristupa, standarda i praksi nadzora nad obavještajnim službama.

Dakle, naglasak u ovom priručnik nije na apstraktnoj akademskoj analizi, već na predstavljanju praktičnih smjernica onima koji nadziru i/ili su redovno u interakciji sa sistemima nadzora nad obavještajnim službama. Iz toga razloga smo izabrali da koristimo format priručnika, sa fokusom na praktične primjere i specifične preporuke koje odražavaju prakse u cijelom svijetu.

1.2 PITANJA KOJIMA SE BAVI PRIRUČNIK

Devet poglavlja u ovom priručniku čine odvojene uvode u važna pitanja vezana za nadzor nad obavještajnim službama (vidjeti Tabelu 1). Svaka je napisana tako da se može zasebno čitati.

1.3 CILJNA PUBLIKA

TOvaj priručnik namijenjen je prvenstveno onima koji su direktno ili indirektno uključeni u nadzor nad obavještajnim službama. Takva publika uključuje predstavnike izvršne, zakonodavne i sudske grane vlasti i njihove uposlenike; obavještajne službenike; predstavnike civilnog društva i predstavnike medija.

Vjerujemo da je sadržaj ovog priručnika od šireg javnog interesa. Ipak, postoje određene grupacije u društvu za koje će ova poglavlja biti posebno korisne. Na primjer, budući da one pobliže razmatraju uloge parlamenta i stručnih nadzornih tijela, za pripadnike i uposlenike tih institucija informacije u ovom priručniku bit će osobito relevantne. Slično, novinari i predstavnici civilnog društva, čiji rad obuhvata analizu obavještajnih službi, naći će u ovim poglavljima mnogo toga korisnog, kao što je to slučaj i sa vladinim službenicima, koji su trenutno angažirani na izradi ili reformiranju sistema nadzora nad obavještajnim službama.

TABELA 1: PREGLED PRIRUČNIKA ZA NADZOR NAD OBAVJEŠTAJNIM SLUŽBAMA

Poglavlje	Naslov	Glavna pitanja kojima se bavi
1	Uvod u nadzor nad obavještajnim službama	▪ Šta je nadzor nad obavještajnim službama? ▪ Zašto je važan nadzor nad obavještajnim službama? ▪ Koje su odgovornosti raznovrsnih institucija uključenih u nadzor nad obavještajnim službama?
2	Uspostava učinkovitih sistema nadzora nad obavještajnim službama	▪ Koje su prednosti i nedostaci raznih institucionalnih pristupa nadzoru nad obavještajnim službama? ▪ Koje su prepreke učinkovitom nadzoru i kako se one mogu rješavati? ▪ Koja su osnovna razmatranja kada se osmišljava pravni i institucionalni okvir za nadzor nad obavještajnim službama?
3	Transparentnost, tajnovitost i nadzor nad obavještajnim službama u demokratijama	▪ Koja je prava ravnoteža između tajnosti i transparentnosti obavještajnih službi u demokratijama? ▪ Šta je dobra praksa u vezi sa zakonima o zaštiti i pristupima informacijama? ▪ Koje su potrebe za obavještajnim informacijama parlamenta, specijaliziranih nadzornih tijela i javnosti?
4	Provođenje nadzora	▪ Koje pristupe i metode koriste nadzorna tijela da bi učinile obavještajne službe odgovornim? ▪ Kako nadzorna tijela mogu provoditi učinkovite istrage o praksama obavještajnih službi? ▪ Kako nadzorna tijela mogu izvještavati o svojim istragama?
5	Nadzor nad prikupljanjem	▪ Zašto je nadzor nad procesom prikupljanja informacija važan? ▪ Kako nadzorna tijela mogu učinkovito pratiti proces prikupljanja informacija? ▪ Koje su prepreke učinkovitom nadzoru nad procesom prikupljanja informacija i kako se one mogu rješavati?
6	Nadzor nad korištenjem ličnih podataka	▪ Zašto je važan nadzor nad korištenjem ličnih podataka? ▪ Kako nadzorna tijela mogu osigurati da obavještajne službe koriste lične podatke samo na načine koji su u skladu sa zakonom? ▪ Koje su prepreke učinkovitom nadzoru nad korištenjem ličnih podataka i kako se one mogu rješavati?
7	Nadzor nad razmjenom informacija	▪ Zašto je važan nadzor nad razmjenom informacija? ▪ Koju ulogu treba da igraju nadzorna tijela u pogledu razmjene informacija? ▪ Koje su prepreke učinkovitom nadzoru nad domaćom i međunarodnom razmjenom informacija i kako se to može rješavati?
8	Finansijski nadzor nad obavještajnim službama	▪ Zašto je važan nadzor nad finansijama obavještajnih službi? ▪ Šta je potrebno da bi obavještajne službe bile finansijski odgovorne? ▪ Koje su uloge i odgovornosti raznih institucija uključenih u finansijski nadzor nad obavještajnim službama?
9	Rješavanje žalbi o obavještajnim službama	▪ Zašto su važni mehanizmi rješavanja žalbi? ▪ Koji tipovi sistema rješavanja žalbi postoje? ▪ Kako se mogu poboljšati sistemi rješavanja žalbi?

2. ŠTA JE NADZOR NAD OBAVJEŠTAJNIM SLUŽBAMA?

Ovo poglavlje predstavlja opseg i sadržaj nadzora nad obavještajnim službama i razmatra institucije koje su u to uključene. Prije nego što nastavimo, međutim, važno je razjasniti šta se podrazumijeva pod terminom *obavještajna služba*.[1] Pošto različite nadležnosti strukturiraju rad obavještajnih službi na različit način, ovaj priručnik koristi funkcionalni pristup definiranju pojma *obavještajna služba*. Tako, on definira obavještajnu službu kao državnu organizaciju koja prikuplja analizira i diseminira informacije u pogledu prijetnji za nacionalnu sigurnost.

Takva definicija obuhvata cijeli niz organizacija — uključujući vojne obavještajne službe, policijske obavještajne službe te civilne obavještajne službe, kako „domaće" – one koje rade u matičnoj državi, tako i „strane" – one koje rade u inostranstvu. Ona, također, uključuje i često zanemarene organizacije koje se obično nalaze u ministarstvu finansija i trezora, kao što su agencije sa zadatkom istraga finansiranja terorista i/ili sprječavanja pranja novca. Kao što se navodi u OECD DAC-ovom *Priručniku o reformi sigurnosnog sektora*: "Većina zemalja ima cijeli niz obavještajnih organizacija koje imaju specifične, ponekad preklapajuće odgovornosti. One uključuju unutrašnje i vanjske obavještajne službe, taktičke i strateške obavještajne službe, kriminalističke obavještajne službe, agencije specijalizirane za prikupljanje podataka iz određene vrste izvora (na primjer, komunikacije, ljudski izvore i slike), civilne i vojne obavještajne službe, te tijela za strateške procjene."[2] Uzete zajedno, te agencije čine „obavještajnu zajednicu".

Obavještajne službe mogu se razlikovati od drugih vladinih agencija i po specijalnim ovlastima koje posjeduju u pogledu prikupljanja informacija - kao što je ovlast da presreću informacije, ovlast da provode tajno praćenje i nadzor, ovlast da koriste prikrivene doušnike, i ovlast da ulaze potajno u privatni posjed. U nekim državama (kao što su Danska, Malezija, Rusija i Švedska), obavještajne službe imaju i policijske ovlasti te se, stoga, ponekad nazivaju „policijske sigurnosne službe" ili „specijalni ogranci". U drugim državama, rad policijskih službi potpuno je odvojen od rada obavještajnih službi: te službe nemaju nikakve policijske ovlasti (npr. da hapse, pritvaraju ili ispituju osumnjičene).

Mada definicija koju mi koristimo ograničava obavještajne službe na državne organizacije, postoje zemlje u kojima vlada angažira privatne firme za obavljanje obavještajnog rada.[3] Kako se nadzor nad privatnim firmama znatno razlikuje od nadzora nad javnim službama, njega nećemo razmatrati u ovom priručniku.

2.1 OPSEG NADZORA NAD OBAVJEŠTAJNIM SLUŽBAMA

Nadzor je sveobuhvatni pojam koji obuhvata *ex ante* nadzor, tekuće praćenje, i *ex post* reviziju, kao i procjenu i istragu. Obavljaju ga rukovodioci u obavještajnim službama, zvaničnici u izvršnoj vlasti, predstavnici sudstva i članovi parlamenta, nezavisne institucije ombudsmena, revizorske institucije, specijalizirana nadzorna tijela, novinari i predstavnici civilnog društva.

Nadzor treba razlikovati od *kontrole* zato što ovaj drugi termin (poput menadžmenta) podrazumijeva ovlast da se usmjeravaju politike i aktivnosti jedne organizacije. Dakle, *kontrola* je tipično povezana sa izvršnom granom vlasti a specifično sa višim rukovodstvom obavještajnih službi. Primjer kontrole, nasuprot nadzoru, bio bi izdavanje izvršnog naloga koji od obavještajne službe zahtijeva da prihvati novi prioritet, kao što je borba protiv

terorizma. Čitaoci treba da budu svjesni, međutim, da svaka vlada ne pravi jasnu razliku između nadzora i kontrole. Iz toga razloga, neke institucije koje su u ovom priručniku opisane kao nadzorna tijela mogu imati i izvjestan broj kontrolnih ovlaštenja.

Glavna svrha nadzora je da obavještajne službe učini odgovornim za svoje politike i akcije u pogledu zakonitosti, ispravnosti, učinkovitosti i efikasnosti.[4] Proces u kojem nadzorno tijelo utvrđuje odgovornost obavještajne službe najčešće ima tri različite faze:

1. nadzorno tijelo prikuplja informacije o obavještajnoj službi;
2. na osnovu prvih informacija, nadzorno tijelo vodi dijalog sa obavještajnom službom;
3. nadzorno tijelo izdaje nalaze i preporuke.

Tako, da bi nadzorno tijelo bilo učinkovito, ono mora imati ovlaštenja da pristupi relevantnim informacijama, da ispita obavještajne službenike, te da izda nalaze i preporuke na osnovu saznanja do kojih dođe. Bez te tri ovlasti ne može biti stvarne odgovornosti, a nadzor nad obavještajnom službom će vjerovatno biti promašaj.

Nadzor može obuhvatiti ne samo ispravnost i zakonitost aktivnosti neke službe, već i njenu učinkovitost i efikasnost. U tom kontekstu, *ispravnost* se odnosi na to da li su akcije obavještajne službe moralno opravdane, dok se *zakonitost* odnosi na to da li su one u skladu sa važećim zakonom. *Učinkovitost* se odnosi na to u kojoj mjeri je služba ostvarila svoje ciljeve, dok *efikasnos*t mjeri koliko ekonomično služba ispunjava postavljene ciljeve. U nekim državama, tijela za nadzor nad obavještajnim službama bave se isključivo zakonitošću (na primjer, Holandski odbor za razmatranje obavještajnih i sigurnosnih službi); u drugim državama, zakon daje mandat nadzornim tijelima da se isključivo usmjere na učinkovitost i efikasnost (na primjer, Odbor za obavještajnu sigurnost u Ujedinjenom Kraljevstvu).

2.2 INSTITUCIONALNA ODGOVORNOST

Učinkovit nadzor nad obavještajnim službama zahtijeva ne samo koordinirane aktivnosti nekoliko državnih tijela, već i aktivno praćenje ponašanja vlade od strane predstavnika civilnog društva i medija. Mada sva ta tijela igraju važnu ulogu, pažnja priručnika je usmjeren prvenstveno na parlamentarna i stručna nadzorna tijela, zato što ta tijela nisu odgovorna ni pred obavještajnim službama, niti pred izvršnom vlasti, što znači da su bolje pozicionirana da nezavisno štite demokratsku odgovornost i poštivanje vladavine zakona i ljudskih prava.

Tabela 2. nudi pregled odgovornosti koje javna i privatna tijela imaju u procesu nadzora. Čitaoci treba da znaju, međutim, da različite države na različite načine upravljaju rečenim odgovornostima, te da sistem nadzora određene države možda ne uključuje sve odgovornosti identificirane u ovoj tabeli.

TABELA 2: NADZORNA TIJELA I NJIHOVE KLJUČNE ODGOVORNOSTI	
Nadzorna tijela	Ključne odgovornosti
Više rukovodstvo obavještajnih službi	▪ Provedba i praćenje pridržavanja internih kontrola; ▪ Jačanje institucionalne kulture koja promovira poštivanje vladavine prava i ljudskih prava; ▪ Razmatranje zahtjeva za korištenjem specijalnih ovlasti i njihovo podnošenje vanjskim tijelima za dobivanje potrebne dozvole za njihovu upotrebu; ▪ Osiguravanje saradnje sa unutrašnjim i vanjskim nadzornim tijelima; ▪ Staranje o provođenju pravila koja zabranjuju nezakonite naloge i podrška službenicima koji odbijaju da ih primjenjuju; ▪ Primjena i praćenje procedura za zaštitu uposlenika koji upozoravaju na nepravilnosti u službi (tzv. „zviždači“).
Izvršna vlast	▪ Imenovanje višeg rukovodstva obavještajne službe; ▪ Uspostava politika i prioriteta za obavještajnu službu, te utvrđivanje smjernica; ▪ Podnošenje izvještaja parlamentu o aktivnostima obavještajnih službi; ▪ Osiguravanje da obavještajne službe sarađuju sa drugim tijelima za nadzor nad obavještajnim službama; ▪ Utvrđivanje budžeta obavještajnih službi i provjera njihovih rashoda; ▪ Odobravanje saradnje obavještajne službe sa drugim službama i agencijama, kako domaćim tako i stranim; ▪ Davanje saglasnosti na zahtjeve za korištenje specijalnih ovlasti; ▪ Odobravanje osjetljivih obavještajnih operacija.
Parlamentarna i stručna nadzorna tijela	▪ Usvajanje, izmjena i dopuna sveobuhvatnog pravnog okvira za rad obavještajnih službi i njihov nadzor; ▪ Procjena ispravnosti, zakonitosti, učinkovitosti i efikasnosti obavještajne službe; ▪ Odobravanje i revizija budžeta obavještajne službe.
Sudstvo	▪ Davanje prethodne saglasnosti i/ili naknadne provjere korištenja posebnih ovlasti od strane obavještajnih službi; ▪ Suđenja u slučajevima krivičnog, građanskog, ustavnog i upravnog prava koji se tiču aktivnosti obavještajnih službi; ▪ Učešće u radu stručnih nadzornih tijela u svojstvu članova i nezavisnih ad hoc istraga u ličnom svojstvu
Institucije ombudsmana	▪ Prijem žalbi protiv obavještajnih službi; ▪ Pokretanje konkretnih istraga o aktivnosti obavještajne službe.
Glavne revizorske institucije	▪ Utvrđivanje nezakonitosti, neefikasnosti i neučinkovitosti u finansijskom upravljanju, te davanje preporuka za njegovo poboljšanje; ▪ Izvještavanje parlamenta o preciznost i pravilnost vladinih računa, utičući na taj način izvršna vlast ispunjava volju parlamenta; ▪ Uvjeravanje javnosti da se njen novac troši zakonito, ispravno, ekonomično i učinkovito.
Civilno društvo i mediji	▪ Preispitivanje politika i aktivnosti obavještajnih službi i tijela za nadzor nad obavještajnim službama; ▪ Razotkrivanje nepravilnog, nezakonitog, neekonomičnog ili neučinkovitog rada obavještajnih službi; ▪ Redovno obavještavanje javnosti o politikama i aktivnostima obavještajnih službi, kao i nadzora nad njima; ▪ Podsticanje javne debate o politikama i aktivnostima obavještajnih službi, te o radu tijela za nadzor nad njima.

2.2.1 Više rukovodstvo obavještajnih službi

Učinkovit nadzor nad obavještajnim službama počinje sa učinkovitim unutrašnjom kontrolom. Zvaničnici izvršne vlasti, članovi parlamentarnih odbora i stručnih tijela nailazit će na teškoće u ispunjavanju svojih nadzornih zadataka ako je više rukovodstvo obavještajne službe nezainteresirano i/ili nekooperativno. S druge strane, ukoliko je više rukovodstvo zainteresirano te daje podršku unutrašnjoj kontroli, onda unutrašnja kontrola, ali i sam sistem upravljanja službom mogu predstavljati važne mehanizme protiv zloupotrebe ovlasti i kršenja ljudskih prava.

Provedba i praćenje pridržavanja mehanizmima unutrašnje kontrole

Više rukovodstvo ima direktnu odgovornost za razvoj i poštivanje unutrašnjih mehanizama kontrole – što je Venecijanska komisija definirala kao „strukture odlučivanja osmišljene tako da osiguraju da su mjere i politike odobrene na ispravan način.“[5] Drugim riječima, unutrašnja kontrola čini obavještajne službenike odgovornim za njihovo ponašanje unutar zakonskog mandata njihovih službi, prioriteta koje izvršna vlast postavi za te službe, kao i politika i propisa koje utvrdi više rukovodstvo službe. Unutrašnja kontrola također uključuje procedure za ispravno utvrđivanje budžeta i vođenje evidencije službi.

Jačanje institucionalne kulture koja promovira poštivanje vladavine prava i ljudskih prava

Potreba da obavještajne službe jačaju i održavaju ”institucionalnu kulturu” koja poštuje vladavinu zakona i ljudska prava u velikoj je mjeri općepriznata.[6] Zakoni i propisi koji promoviraju takvu kulturu su, stoga, važni, ali ne i dovoljni. Više rukovodstvo službe mora također razviti i provoditi programe koji su osmišljeni tako da uposlenici službe prihvate i interioriziraju vrijednosti ustavnosti, zakonitosti , odgovornosti i integriteta.

Razmatranje zahtjeva za korištenjem specijalnih ovlasti i njihovo podnošenje vanjskim tijelima za dobivanje potrebne dozvole za njihovu upotrebu

U većini država, korištenje specijalnih ovlasti od strane obavještajne službe je u krajnjoj instanci podložno odobrenju ministra i/ili suda zbog posljedica koje takve ovlasti mogu imati na ljudska prava. Više rukovodstvo službe, međutim, igra ključnu ulogu u donošenju odluke o tome koji zahtjevi zaslužuju da budu upućeni tim vanjskim tijelima. Rukovodstvo treba da donosi takve odluke u kojima će se uspostaviti ravnoteža između specijalnih mjera i prirode same prijetnje. Veći rizici za ljudska prava treba da nalažu više nivoe unutrašnje saglasnosti.

Osiguravanje saradnje sa unutrašnjim i vanjskim nadzornim tijelima

Više rukovodstvo službe je odgovoran za učinkovito funkcioniranje svih unutrašnjih nadzornih tijela. Ta odgovornost uključuje osiguravanje da uposlenici službe u potpunosti sarađuju sa unutrašnjim ali i sa vanjskim nadzornim tijelima. Nadalje, više rukovodstvo treba da izolira (pogotovo unutrašnja) nadzorna tijela od administrativnih poslova tako da mogu funkcionirati učinkovito kao mehanizam za rješavanje žalbi.

Staranje o provođenju pravila koja zabranjuju nezakonite naloge i podrška službenicima koji odbijaju da ih primjenjuju

Više rukovodstvo mora preduzeti sve potrebne radnje kako bi osiguralo da se ne izdaju nezakoniti nalozi, a ukoliko se kojim slučajem izdaju, da se ne primjenjuju. Ovo može biti

osnaženo zakonima za zaštitu tzv. „zviždača“, koji omogućavaju uposlenicima obavještajne službe da prijave informaciju koja ukazuje na nepropisno ponašanje spoljnim ili vanjskim tijelima, koja su za to određena. U nekim državama, uspostavljene su zakonske procedure za izvještavanje direktora obavještajne službe ili drugog relevantnog zvaničnika o upitnoj obavještajnoj aktivnosti. U Bosni i Hercegovini, sporna aktivnost se prijavljuje generalnom inspektoru službe (vidjeti Okvir 1). U drugim zemljama, prijavljuje se odgovornom ministru.[7] Usto, domaći zakoni nekih država (kao što je Bugarska[8]) smatraju službenike obavještajnih službi individualno odgovornim za nezakonite radnje i/ili za kršenja službene dužnosti.

Okvir 1: Dužnost obavještajnih službenika da prijavljuju nezakonitu aktivnost u Bosni i Hercegovini

„Ukoliko zaposleni smatra da je primio nezakonitu naredbu, svoju zabrinutost u pogledu nezakonitosti saopćava naredbodavcu. U slučajevima kada naredbodavac ponovi naredbu, zaposleni traži pismenu potvrdu te naredbe. Ukoliko zaposleni i dalje ima određene rezerve, prosljeđuje naredbu neposrednom rukovodiocu naredbodavca i o tome obavještava glavnog inspektora.”[9]

2.2.2 Izvršna vlast

Doktrina ministarske odgovornosti[10] propisuje da je svaki ministar odgovoran šefu države, vladi i parlamentu za provođenje svojih ovlasti i funkcija.[11] Prema toj doktrini, izvršna vlast, koja utvrđuje politiku obavještajne službe, politički je odgovorna za njeno ponašanje.

Uobičajeno je da obavještajne službe podnose izvještaje vladinom ministru koji je odgovoran za osiguravanje da služba funkcionira na ispravan, zakonit, učinkovit i ekonomičan način. U Njemačkoj, na primjer, vanjska, domaća i vojna obavještajna služba podnose izvještaje šefu Savezne kancelarije, ministru unutrašnjih poslova i ministru odbrane.[12]

Stepen kontrole koju provodi izvršna vlast varira od države do države. Kompleksnost obavještajnog rada može otežati izvršnoj vlasti praćenje i kontrolu nad aktivnostima službe. Uistinu, „sam po sebi, monopol specijaliziranog znanja koji posjeduje agencija,“ kako je zapazila Venecijanska komisija, „agenciji će u praksi osigurati značajan stepen autonomije od kontrole vlade.”[13]

Mada zvaničnici izvršne vlasti imaju veliki interes da spriječe obavještajne promašaje, oni nisu podjednako zainteresirani da ih javno razotkriju, onda kada se oni dese. Javno razotkrivanje grešaka ili nepravilnosti službe može izazvati političko sramoćenje i negativno utjecati na karijere tih ministara. Iz tog razloga, neki stručnjaci nemaju povjerenje u sposobnost izvršne vlasti da obavlja odgovarajući nadzor nad obavještajnim službama te se, umjesto toga, oslanjaju na praćenje i kritiku odluka izvršne vlasti od strane parlamenta, sudstva i civilnog društva.

Unatoč ovoj zabrinutosti, izvršna vlast ipak utjelovljuje važnu kariku u lancu odgovornosti. Odgovornosti navedene u Tabeli 2. jasno ukazuju na to da, uz političke, izvršna vlast ima i operativnu odgovornost u pogledu obavještajnih službi, pogotovo u vezi sa provedbom politike. Iz tog je razloga važno da se informacije koje se odnose na teške ili osjetljive operativne odluke ne sakrivaju od izvršne vlasti. Naprotiv, izvršna vlast treba uvijek biti informirana.

2.2.3 Parlamentarna i stručna nadzorna tijela

Jednako kao što je bitno uspostaviti i sprovoditi učinkovit nadzor izvršne vlasti nad sigurnosnim obavještajnim aktivnostima, od ključnog je značaja imati i nezavisni nadzor – kako parlamentarni, tako i neparlamentarni. Na potrebu za učinkovitim nadzorom nad obavještajnim službama od strane tijela nezavisnih od aktuelne vlade ukazuje mnogo činjenica, a ponajviše tajnost obavještajnog rada, pomanjkanje sudske provjere, pretjerana upotreba tajnih nadzornih tehnika koja predstavljaju prijetnju za ljudska prava, te evidencije ranijih prijestupa.[14]

Općenito, parlamentarna i stručna nadzorna tijela osiguravaju najučinkovitiji vanjski nadzor. Ova prva se mogu podijeliti u dvije kategorije: generalni odbori sa širokim mandatom (kao što su odbori za odbranu i vanjske poslove) i specijalizirani odbori, čiji jedini fokus je obavještajna zajednica. Mada generalni odbori (posebno u područjima budžeta i finansija) mogu imati posebne nadzorne odgovornosti u pogledu obavještajnih službi, najveći dio nadzora nad obavještajnim službama obično se provodi u specijaliziranim odborima. To ponajprije zbog većeg iskustva i stručnosti članova ovih odbora, te stoga što takav pristup ograničava krug znanja i informacija na članove odbora, umjesto na sve članove parlamenta.

Stručna tijela za nadzor nad obavještajnim službama (ponekad se zovu i „specijalizirane nadzorne institucije“ ili „specijalizirana vanparlamentarna nadzorna tijela“) uspostavljaju se i funkcioniraju nezavisno od izvršne vlasti, parlamenta i obavještajnih službi za koje imaju mandat da ih nadziru. Stručna tijela za nadzor imaju koristi od stručnog znanja svojih članova i mogućnosti da usmjere pažnju rada na jednu oblast. U većini država, takva tijela čine obavještajni stručnjaci, kao što su bivše ili sadašnje sudije, tužioci i šefovi policijskih službi.[15] Doista, članovi stručnih nadzornih tijela često imaju veće iskustvo i stručno znanje od članova specijaliziranih parlamentarnih odbora. Nadalje, članovi stručnih tijela obično imaju slobodu da se u potpunosti posvete nadzoru nad obavještajnim službama, dok parlamentarci obično sjede u nekoliko odbora te stoga imaju višestruke odgovornosti. Druga prednost stručnih nadzornih tijela je da njihovi članovi nisu profesionalni političari, niti su direktno uključeni u svakodnevnu političku aktivnost, te je time njihovo ponašanje obično manje ispolitizirano nego u slučaju parlamentaraca. Ipak, stručni nadzor treba uvijek biti posmatran kao komplementaran, a ne kao zamjena za parlamentarni nadzor pošto principi demokratskog upravljanja zahtijevaju direktnu kontrolu svih vladinih operacija od strane parlamenta.

Neke države (kao što je Australija, vidjeti Okvir 2) su dodatno pojačale nadzor nad obavještajnim službama uspostavivši ured nezavisnog generalnog inspektora. Naziv, mandat, ovlasti i funkcije ovog ureda znatno se razlikuju od države do države (vidjeti Farson –Poglavlje 2), ali njegove ključne misije obično uključuju osiguravanje da obavještajne službe poštuju ustav, relevantne zakone i operativne politike koje utvrdi izvršna vlast. Druge zajedničke funkcije uključuju:

- obrazovanje službenika obavještajne službe o njihovim pravima i odgovornostima;
- provođenje internih revizija i inspekcija, pogotovo u svrhu otkrivanja i sprječavanja neodgovornog trošenja novca, prevara i zloupotrebe;
- osiguravanje provođenja učinkovitih sigurnosnih politika i procedura;
- prijem žalbi i istrage po žalbama koje ulože radnici službe;
- osiguravanje da se objave informacije na koje, na osnovu zakona o slobodi informacija, javnost ima pravo;

- osiguravanje da službe vode evidencije podataka u skladu sa relevantnim zakonima i politikama.[16]

Okvir 2: Australijski generalni inspektor za obavještajne službe i sigurnost

Australijski generalni inspektor (GI) za obavještajne i sigurnosne službe je odgovoran premijeru, višim ministrima, i parlamentu za zakonito i ispravno postupanje obavještajne službe zemlje i drugih sigurnosnih agencija. On to čini tako što istražuje rad obavještajnih službi i sigurnosnih agencija, te izvještava o njihovim aktivnostima. Mandat GI-ja potom uključuje odgovornost za praćenje da li obavještajne službe i sigurnosne agencije djeluju učinkovito, te da li poštuju ljudska prava.

Kako bi ispunio ovaj mandat, GI ima ovlast po australijskom zakonu da provodi istrage na zahtjev odgovornog ministra ili, pak, na vlastitu inicijativu. Usto, GI ima ovlast da prima i istražuje žalbe koje ulažu pojedinci koji smatraju da su im prava ugrožena aktivnostima obavještajne službe. Takve istrage mogu uključiti inspekciju prostorija obavještajne službe (kao što su mjesta pritvora), uzimanje svjedočenja pod zakletvom i pristup dokumentima. Po zaključenju svake istrage, GI podnosi izvještaj nadležnom ministru, čiji sažetak je najčešće sastavni dio godišnjeg izvještaja GI-a australijskom parlamentu. Direktor date službe i odgovorni ministar zakonom su obavezni da GI-u podnose izvještaj o provedbi bilo kojih preporuka koje su sadržane u njegovom izvještaju.[17]

Mandat parlamentarnih odbora za nadzor i stručnih nadzornih tijela varira od države do države. Neke zemlje (poput Sjedinjenih Država, sa kongresnim odborima za nadzor nad obavještajnim službama) imaju mandat koji obuhvata cijeli spektar od ispravnog rada, zakonitosti, učinkovitosti i efikasnosti;; druge (poput Holandije i Švedske) ograničavaju mandat tih tijela isključivo na zakonitost.

Kako bi mogli ispuniti date mandate, parlamentarni odbori za nadzor i stručna nadzorna tijela često imaju velike ovlasti, koje mogu uključiti sve ili tek poneke sa ove (nepotpune) liste:

- ovlast da pristupe klasificiranim informacijama;
- ovlast da dobivaju i razmatraju godišnje i druge izvještaje obavještajnih službi;
- ovlast da nalože zvaničnicima izvršne vlasti i obavještajnih službi da svjedoče pod zakletvom (eng. subpoena);
- ovlast da pozovu vanjske stručnjake i druge predstavnike javnosti da svjedoče pod zakletvom;
- ovlast da se periodično sastaju sa odgovornim ministrima i/ili direktorima službi;
- ovlast da provode kako redovne, tako i *ad hoc* inspekcije, te da posjećuju prostorije obavještajnih službi

2.2.4 Sudstvo

Pošto obavještajne službe nisu iznad zakona, one potpadaju pod jurisdikciju sudova. Mada uloga sudova u pogledu obavještajnog rada zaslužuje detaljniju pažnju nego što joj se može ovdje posvetiti, sljedeći kratki komentari mogu biti od koristi.

Mada sudstvo ima odgovornost da održava vladavinu prava i osigura poštivanje ljudskih prava, sudije tradicionalno prepuštaju izvršnoj vlasti pitanja nacionalne sigurnosti iz dva razloga. Prvo, ustavi i vladajući zakoni često pitanja nacionalne sigurnosti stavljaju pod isključivu ovlast izvršne vlasti. Drugo, mnoge sudije doživljavaju sudove kao mjesta na kojima nije poželjno otkrivanje povjerljivih informacija.[18] Unatoč tome, neki sudski sistemi igraju aktivnu ulogu u nadzoru nad obavještajnim službama. U Sjedinjenim Državama, na primjer, proširenje prava krivično optuženih u pogledu garancija za pravičan sudski proces je dovelo do toga da sudije sve detaljnije razmatraju postupke vlasti. Usto, vidan je trend da Kongres usvaja sve više zakona koji se tiču obavještajnih službi, što je također doprinijelo povećanoj sudskoj kontroli.[19] U drugim zemljama, posebno tamo gdje izvršna vlast postavlja pretjerane i prevelike zahtjeve u ime nacionalne sigurnosti, sudije su sve aktivnije u odbrani ustavnih i ljudskih prava.[20]

Sudski nadzor nad obavještajnim službama odvija se na četiri glavna načina, od kojih tri prevazilaze nadzor i zalaze u područje kontrole. Prvo, zakoni koji su na snazi često zahtijevaju od obavještajnih službi, koje žele da koriste specijalne istražne mjere (kao što je presretanje komunikacije), da dobiju prethodno odobrenje od sudije ili da te mjere budu podložne naknadnoj sudskoj provjeri. Takvi zahtjevi su važni zato što nameću nazavisnu provjeru zakonitosti onih aktivnosti službe koje u znatno većoj mjeri ograničavaju ljudska prava od uobičajenih mjera. Drugo, sudije mogu biti pozvane da predsjedavaju suđenjima za krivična djela koja se odnose na obavještajni rad, te da presuđuju u predmetima – ustavnim, građansko-pravnim ili upravnim - koji se tiču pitanja vezanih za obavještajni rad. Treće, u nekim državama (kao što je Francuska), istražne sudije, specijalisti za sigurnosna pitanja, mogu dobiti kontrolnu ulogu nad istragama koje sprovode obavještajne službe. Četvrto, sudije ponekad mogu postati članovi nadzornih tijela, ili, pak, mogu biti pozvani da predsjedaju *ad hoc* istražnim komisijama.

Prve tri od navedenih uloga kvalificiraju se kao sredstva kontrole pošto sudijama daju ovlasti da usmjeravaju aktivnosti obavještajnih službi. U poređenju sa njima, četvrta uloga je ograničena jer obično ne daje ovlasti izdavanja obavezujućih preporuka.

2.2.5 Institucije ombudsmena

Najčešća interakcija između institucije ombudsmena i obavještajne zajednice se odvija kroz rješavanje žalbi koje protiv obavještajnih službi podnose predstavnici javnosti. U Holandiji, na primjer, svako može podnijeti žalbu državnom ombudsmenu po pitanjima vezanim za „djelovanje ili navodno djelovanje nadležnih ministara, šefova [obavještajnih] službi, koordinatora, te osoba koje rade za te službe i za koordinatora".[21] Podnosilac žalbe mora najprije obavijestiti nadležnog ministra, koji potom traži savjet od Odbora za nadzor obavještajnih i sigurnosnih službi (CTIVD). Potom, državni holandski ombudsmen istražuje žalbu i donosi „svoju odluku o žalbi u pisanom obliku osobi koja je podnijela žalbu i, u onoj mjeri u kojoj sigurnost ili drugi vitalni interesi države drugačije ne nalažu, navodi svoje razloge".[22]

Institucije ombudsmena treba da budu nezavisne i da im je zakonom omogućen pun pristup informacijama bitnim za njihove istrage. Nažalost, one nerijetko imaju premalo uposlenika da bi mogli učinkovito pokriti široke nadležnosti, koja često obuhvataju ne samo obavještajnu zajednicu, već i oružane snage, a ponekad i cijelu vladu. Stoga, institucije ombudsmena često nisu sposobne posvetiti dovoljno stručnog znanja niti resursa nadzoru nad obavještajnim službama.

2.2.6 Glavne revizorske institucije

Poput institucije ombudsmena, glavne revizorske institucije (GRI) vrše nezavisne, vanjske provjere djelovanja obavještajnih službi. One posebno prate finansijske aspekte obavještajnog rada, procjenjuju da li je evidencija službe ispravna i tačna, da li unutrašnja kontrola rashoda funkcionira ispravno, te da li su rashodi službe u skladu sa važećim propisima (vidjeti Poglavlje 8 – Wills). Pored tih odgovornosti, GRI nekada rade procjene svrsishodnosti troškova, odnosno da li je prilikom nabavke dobara i usluga ostvaren dobar odnos cijene i kvaliteta (eng. value-for-money), a sve u cilju što boljeg informiranja zakonodavca i izvršne vlasti kako bi oni mogli na najbolji način strukturirati budžete i odrediti prioritete obavještajne službe.

2.2.7 Civilno društvo i mediji

Iako je civilno društvo amorfan koncept, njegovo općeprihvaćeno shvaćanje je da je to skup autonomnih organizacija koje postoje u javnom domenu između institucija države i privatnog života pojedinca i zajednica. Ova definicija uključuje, na primjer, akademsku zajednicu, nevladine organizacije (NVO), grupe za zagovaranje te vjerske zajednice. Velika prednost organizacija civilnog društva u provođenju nadzora nad obavještajnim službama je mogućnost da neograničeno analiziraju i kritiziraju politike vlade.

Kao i organizacije civilnog društva, medijske organizacije koriste nezavisno (odnosno, nevladino) stručno znanje kako bi informirale o aktivnostima obavještajnih službi. Istraživački novinari, pogotovo, igraju ključnu ulogu u razotkrivanju neispravnog, nezakonitog, neefikasnog i/ili neučinkovitog djelovanja obavještajnih službi. Jednom razotkriveni, ti slučajevi neuspjeha ili grešaka često postaju predmet formalnih istraga koje provode parlamentarni odbori ili druga nezavisna nadzorna tijela, kao što su stručna nadzorna tijela, institucije ombudsmena ili glavne revizorske institucije (SAI). Bez medijskih izvještaja koji skreću pažnju na te probleme, ti slučajevi možda nikad ne bi bili istraženi.

Bilo da je to u cilju razotkrivanja nepravilnosti ili, pak, zato što traže odgovornost nosilaca organa izvršne vlasti, mediji svojim izvještavanjem čine ove probleme temama javne debate te na taj način one postaju teme dnevnog reda vlade. Na primjer, u serija članaka *Top Secret America dnevni list Washington Post* objavio je podatke o zapanjujućem širenju obavještajne zajednice u Sjedinjenim Državama u deceniji nakon napada od 11. septembra 2001. godine, čime je pokrenuo žustru javnu debatu o isplativosti i učinkovitosti ovog širenja obavještajne zajednice.[23] Međutim, moramo napomenuti da veoma ispolitizirano ili pristrasno novinarstvo može biti štetno za nadzor nad obavještajnim službama.

2.3 CIKLUS NADZORA NAD OBAVJEŠTAJNIM SLUŽBAMA

Nadzor se može vršiti u nekoliko različitih vremenskih tačaka. Može se desiti na samom početku operacije kada je ona predložena ali još nije poduzeta (nadzor *ex ante*). Nadalje, može se desiti dok je operacija u toku (tekući nadzor), ili se, pak, može desiti nakon što je operacija zaključena (nadzor *ex post*).

2.3.1 Prethodni (*ex ante*) nadzor

Najčešće aktivnosti nadzora *ex ante* uključuju: stvaranje sveobuhvatnog pravnog okvira za obavještajne službe i tijela koja ih nadziru, izrada i odobravanje budžeta za obavještajne službe, te davanje saglasnost za naročito osjetljive obavještajne operacije. Da bi pravni okvir

bio učinkovit, mandati i ovlasti službi, kao i nadzornih tijela moraju biti jasno propisani. Iako ovo nije nadzor u pravom smislu riječi, ova zakonodavna aktivnost je polazište (i ono bez čega ne može) bilo kakvog učinkovitog sistema nadzora. Bez jasno definiranih mandata i ovlasti, obavještajne službe i nadzorna tijela ne mogu funkcionirati na pravi način (izrada pravnog okvira se razmatra opširno u Poglavlju 2 – Farson).

Vladine agencije ne mogu raditi bez sredstava. Tako, parlament, koji u demokratiji kontrolira korištenje javnih sredstava, mora usvojiti godišnje budžete za sve vladine agencije, uključujući obavještajne službe. Nadležni ministar najčešće podnosi prijedlog budžeta nadležnom parlamentarnom odboru, koji to radi u konsultaciji sa višim rukovodstvom službi, ministarstvom finansija i u nekim slučajevima glavnom revizorskom institucijom (budžetski proces se detaljno razmatra u Poglavlju 8 – Wills). Članovi parlamentarnog odbora potom procjenjuju predloženi budžet u odnosu na tekuću realizaciju obavještajne politike. Ne iznenađuje što parlamentarci često koriste budžetski proces kao priliku da kritiziraju izvršnu vlast i prioritete koje je ona odredila za obavještajne službe.

Prethodnu saglasnost za obavještajne aktivnosti je potrebno pribaviti za specijalne ovlasti kojima se ograničavaju prava pojedinaca, kao što su elektronički nadzor ličnih komunikacija. Najčešće, ovaj oblik nadzora *ex ante* provodi sudija, ali u određenim situacijama može ga obavljati i nesudsko ili kvazisudsko nadzorno tijelo, kao što je Komisija G10 njemačkog *Bundestaga*,nazvana prema Članu 10. njemačkog Temeljnog zakona, koji se odnosi na poštansku i telekomunikacijsku privatnost (vidjeti Hutton—Poglavlje 5).

2.3.2 Tekući nadzort

Tekući nadzor može uključiti istrage, inspekcije na licu mjesta, periodična saslušanja, te redovno izvještavanje o aktivnostima obavještajnih službi i samih nadzornih tijela. Usto, u nekim zemljama, sudije periodično razmatraju tekuće operacije prikupljanja informacija, kao što su prisluškivanje telefona, kako bi utvrdili da li je opravdan nastavak tih operacija.

Godine 2011, Holandski odbor za nadzor obavještajnih i sigurnosnih službi (CTIVD) izvijestio je da su njegove tekuće nadzorne aktivnosti uključivale redovno preslušavanje snimaka telefonskih razgovora, sigurnosne provjere službe i obrada zahtjeva za pristupom dosjeima službe. Usto, Odbor za razmatranje istražio je da li su službe ispunile svoju zakonsku obavezu da obavijeste pojedince koji su bili predmet obrade specijalnim istražnim mjerama.[24] Još jedno tijelo za nadzor nad obavještajnim službama sa specifičnim mandatom za provođenje tekućeg nadzora je Norveški parlamentarni odbor za nadzor nad obavještajnim službama (vidjeti Okvir 3).

Okvir 3: Norveški parlamentarni odbor za nadzor nad obavještajnim službama (Odbor EOS)

Aktivnosti Norveškog parlamentarnog odbora za nadzor nad obavještajnim službama (Odbor EOS) su utvrđene u Zakonu od 3. februara 1995, koji se odnosi na praćenje rada obavještajnih sigurnosnih službi. Zakon utvrđuje da je Odbor EOS nadležan isključivo za monitoring obavještajnih službi.[25] Prema tome, „Odbor ne može usmjeravati rad tijela koji je predmet monitoringa niti ta tijela mogu koristiti Odbor za konsultacije".[26]

Član 3. Zakona navodi da Odbor EOS-a "redovno prati prakse obavještajnih, nadzornih i sigurnosnih službi u javnoj i vojnoj upravi". Član 4. dozvoljava Odboru, u ispunjavanju njegovog mandata, da uđe u prostorije, dok Član 5. ovlašćuje Odbor da sasluša svjedoke, koji su obavezni da se pojave na saslušanjima.

Nadalje, Član 8. obavezuje Odbor da „ javno izda izvještaj o žalbi koju dobije, te da izdaje godišnje izvještaje Stortingu (norveškom parlamentu) u kojem opisuje svoje aktivnosti. Usto, Odbor može izdavati periodične izvještaje na određene teme ako se otkriju činjenice o kojima treba biti smjesta upoznat Storting."[27] Ova posljednja ovlast omogućava Odboru EOS-a da provodi važan tekući nadzor nad aktivnostima norveških obavještajnih službi.

2.3.3 Naknadni (*ex post*) nadzor

Najčešći oblici nadzora *ex post* su tematske revizije, revizije slučajeva, revizije rashoda (vidjeti Poglavlje 8 – Wills), te godišnje revizije. U određenim situacijama, međutim, kao što je situacija kada se razotkrije navodni prijestup, nadzor *ex post* može imati oblik *ad hoc* istrage. One se obavljaju sa ciljem detaljnog istraživanja nekog slučaja, na osnovu kojeg se izdaju preporuke.

Na primjer, 2004. godine vlada Kanade pokrenula je specijalnu istragu o ulozi Kraljevske kanadske konjičke policije (RCMP) u slučaju Mahera Arara, kanadskog državljanina čije je hapšenje od strane Sjedinjenih Država i predaja Siriji kao krajnji rezultat imala njegovo mučenje (vidjeti Roach – Poglavlje 7). Istraga je imala dva aspekta: razmatranje činjenica i razmatranje politike. Cilj razmatranja činjenica je bio "istražiti i izvijestiti o akcijama kanadskih zvaničnika u vezi sa onim što se desilo Maheru Araru."[28] Cilj razmatranja politike je bio „da se daju preporuke za uvođenje nezavisnog mehanizma neposrednog nadzora aktivnosti RCMP-a koje se odnose na nacionalnu sigurnost".[29] Strukturiranje istraga ex post na način koji se sastoji iz dva dijela je korisno zato što istovremeno utvrđuje istinu o onome što se desilo, ali i pruža priliku za formuliranje prijedloga praktične politike.

Drugo važno područje naknadnog nadzora je rješavanje žalbi (vidjeti Poglavlje 9 – Forcese),[30] što može biti rađeno kroz nekoliko različitih institucionalnih oblika. Žalbe često rješava sudstvo, ali one, također, mogu biti rješavane i u nesudskim institucijama, kao što su institucije ombudsmena (npr. u Srbiji), parlamentarni odbori (kao što je to slučaj u Mađarskoj), ili stručna nadzorna tijela (kao što je slučaj u Norveškoj).

2.4 PROCJENA NADZORA NAD OBAVJEŠTAJNIM SLUŽBAMA

Tijela za nadzor nad obavještajnim službama procjenjuju rad obavještajnih službi, ali ko ocjenjuje rad nadzornih sistema i kako se taj rad ocjenjuje? Obavještajni nadziratelji i predstavnici akademske zajednice su tek nedavno počeli odgovarati na ta pitanja, zato što, između ostalih faktora, u mnogim državama sistemi nadzora nad obavještajnim službama nisu bili uspostavljeni sve do 1990-ih.

Nekoliko zemalja je svoje sisteme nadzora nad obavještajnim službama podvrgnulo vanjskoj ocjeni. U Kanadi, specijalni odbor Donjeg doma je to uradio kao dio petogodišnje revizije kanadskog Zakona o sigurnosnoj i obavještajnoj službi;[31] dok u Holandiji, na zahtjev CTIVD-a, jedan nezavisni ekspert proveo je sličnu reviziju Zakona o sigurnosno-obavještajnoj službi.[32] Usto, neke zemlje su ocijenile svoje sisteme nadzora kao dio parlamentarnih ili nezavisnih istraga u vezi sa navodnim neuspjesima ili greškama obavještajne službe. Primjeri za to uključuju Komisiju 9/11 u Sjedinjenim Državama i istragu u slučaju Arar u Kanadi.

Sljedeći principi mogu usmjeravati buduća istraživanja ove važne teme, čija je potpuna kompleksnost mimo opsega ovog priručnika:

- Važeći zakon treba da da mandat za periodičnu reviziju sistema nadzora nad obavještajnim službama, kako bi se utvrdilo da li još uvijek odgovara svojoj namjeni;
- Te periodične revizije treba da obuhvate cijeli sistem nadzora – uključujući više rukovodstvo obavještajne službe, izvršnu vlast, parlament, sudstvo, nezavisna nadzorna tijela, civilno društvo i medije;
- Takve revizije treba da utvrde da li mandati tijela za nadzor nad obavještajnim službama, kada se procjenjuju kolektivno, obuhvataju najvažnije aspekte aktivnosti obavještajne službe. Osobito, treba da utvrde da li mandati obuhvataju i zakonitost i učinkovitost rada službe;
- Ocjene specifičnih nadzornih tijela treba da se fokusiraju na sposobnost nadzornog tijela da učini službe koje nadziru odgovornima. Drugim riječima, jesu li ovlasti i resursi nadzornog tijela dovoljni za izvršavanje njihovog mandata? Od posebne je važnosti da li je tijelo dovoljno nezavisno od izvršne vlasti i obavještajnih službi, da li ima pristup klasificiranim informacijama, da li posjeduje potrebne istražne ovlasti, te da li ima dovoljno stručnog osoblja?

3. ZAŠTO JE VAŽAN NADZOR NAD OBAVJEŠTAJNOM SLUŽBOM?

Tri su glavna razloga zbog kojih države stvaraju sisteme nadzora nad obavještajnim službama: jačanje demokratskog upravljanja nad obavještajnim službama (uključujući njihovu odgovornost izbornom tijelu), poštivanje vladavine prava, te osiguravanje učinkovitosti i efikasnosti rada službe.

3.1 DEMOKRATSKA VLADAVINA I ODGOVORNOST

Jedan od temeljnih principa demokratske vladavine je odgovornost državnih institucija prema izbornom tijelu, tj. glasačima. Štaviše, zato što obavještajne službe koriste javna sredstva, javnost ima pravo znati da li se ta sredstva koriste na ispravan, zakonit, ekonomičan i učinkovit način.

S obzirom na povjerljivu prirodu najvećeg dijela obavještajnog rada, obavještajne službe ne mogu biti potpuno transparentne. Tako, društvo mora stvoriti alternativni mehanizam (pored javne kontrole) da bi pratio rad obavještajnih službi u ime glasača. Najčešći mehanizmi su parlamentarni odbori i stručna nadzorna tijela koja formira parlament u ispunjavanju svojih obaveza uspostavljanja odgovarajućih mehanizama kočnica i ravnoteže (eng. checks and balances) prema vladinim agencijama.

Mehanizmi kočnice i ravnoteže vlasti trebaju osigurati, osobito, da obavještajne službe djeluju u svrhu odbrane nacionalne sigurnosti, a ne sigurnosti tekuće vlade. I doista, obavještajne službe ne smiju nikada biti instrument jedne političke partije, već biti sluge javnosti.

Demokratska vladavina može također ojačati povjerenje javnosti u rad obavještajnih službi ako javnost općenito zna da su službe ispravno nadgledane od strane njenih predstavnika u parlamentu i drugih tijela za nadzor obavještajnih službi.

3.2 PODRŠKA VLADAVINI PRAVA

Obavještajne službe, kao bilo koja druga vladina agencija, imaju obavezu poštivati i podržavati vladavinu prava. Čak i postojanje prijetnje za nacionalnu sigurnost nije dovoljan razlog da obavještajna služba krši zakon. Nezakonita aktivnost obavještajne službe ne samo da krši vladavinu prava kojeg je ta služba obavezna štititi, već i službi i vladi umanjuje reputaciju u zemlji i u svijetu. Posebno korištenje specijalnih ovlasti od strane obavještajnih službi treba biti budno praćeno zbog postojanja mogućnosti kršenja ljudskih prava.

U onim zemljama gdje su obavještajne službe historijski povezane sa kršenjem zakona i kršenjem ljudskih prava, budni nadzor je posebno važan, ne samo kako bi se obeshrabrilo ponovno činjenje grešaka, već i da se izgradi povjerenje javnosti u službe i u vladu.

3.3 UČINKOVITOST I EFIKASNOST

Pošto obavještajne službe igraju vitalnu ulogu u zaštiti nacionalne sigurnosti, a njihovi resursi su ograničeni, važno je da oni budu korišteni učinkovito i efikasno, a ne da se nepotrebno troše. Stoga, dobro osmišljen sistem nadzora nad obavještajnim službama treba pratiti da li obavještajne službe zaista koriste svoje resurse na način koji im omogućava da ispune prioritete koje im je postavila izvršna vlast, postižući pritom najveću moguću vrijednost za potrošen novac poreskih obveznika.

Uobičajeno je da efikasnost službe prati i parlament tokom budžetskih saslušanja i glavna revizorska institucija tokom svojih redovnih provjera rashoda. Tajnovita priroda obavještajnog rada olakšava obavještajnim službama (u poređenju sa drugim vladinim agencijama) da prikriju slučajeve prevare i nepotrebnog trošenja. Stoga, nadzorna tijela moraju posebno pažljivo kontrolirati korištenje javnih sredstava (vidjeti Poglavlje 8 – Wills).

4. DOBRE PRAKSE

Svaka država treba osigurati da njene obavještajne službe djeluju na način koji je u skladu sa preuzetim međunarodnim pravnim obavezama, uključujući one koje su utvrđene u Povelji Ujedinjenih nacija i Međunarodnom paktu o građanskim i političkim pravima. Ovisno o mandatu službe, međunarodni sporazumi u pogledu korištenja policijskih ovlasti morali bi također biti primjenjivi.

Jedan način da se ispunjavaju te obaveze je slijediti dobre prakse. U ovom priručniku, pod dobrim praksama se podrazumijevaju domaće i međunarodne pravne odredbe, kao

i domaće institucionalne strukture, procedure i modeli koji promoviraju učinkovit nadzor nad obavještajnim službama.

Pošto ne postoji jedan jedinstveni model za nadzor nad obavještajnim službama, ne može se opravdano tvrditi da su jedan jedinstveni standard ili praksa nedvosmisleno najbolji. Prije se može reći da se raznolikost jednako dobrih modela i pristupa može naći u državama diljem svijeta. Prenošenje dobrih praksi iz jedne države u drugu može biti teško zbog razlika u pravnom, političkom i kulturalnom sistemu. A čak i kada je to moguće, taj proces obično zahtijeva prilagođavanje praksi prije nego što mogu razložno biti primijenjene. Ipak, moguće je identificirati zajedničke standarde i prakse koji doprinose učinkovitom nadzoru nad obavještajnim službama.

DCAF je 2010. godine za specijalnog izvjestioca UN-a za promociju i zaštitu ljudskih prava i temeljnih sloboda prilikom borbe protiv terorizma pripremio katalog dobrih praksi za nadzor nad obavještajnim službama koji se temelji na komparativnoj analizi ustava, zakona, dekreta, parlamentarnih rezolucija, nezavisnih istraga, i sudskih presuda u preko pedeset država. Rezultati ovog istraživanja su sažeti u Okviru 4

Okvir 4: Zbirka dobrih praksi Ujedinjenih nacija u pogledu nadzora nad obavještajnim službama

Na osnovu istraživanja DCAF-a iz 2010. godine, specijalni izvjestilac UN-a za promociju i zaštitu ljudskih prava i temeljnih sloboda prilikom borbe protiv terorizma prezentirao je zbirku dobrih praksi o obavještajnim službama i njihovom nadzoru.[33] Dok ova zbirka uključuje trideset i pet dobrih praksi koje se tiču pravnog osnova, nadzora i odgovornosti, poštivanja ljudskih prava i obavještajnih funkcija, dolje data lista se odnosi samo na dobre prakse vezane za nadzor nad obavještajnim službama.

Praksa 6. Obavještajne službe se nadziru kroz kombinaciju unutrašnjih, izvršnih, parlamentarnih, sudskih i specijaliziranih institucija za nadzor, čiji mandat i ovlasti se temelje na javno dostupnom zakonu. Učinkovit sistem nadzora nad obavještajnim službama uključuje najmanje jednu civilnu instituciju koja je nezavisna i od obavještajnih službi i od izvršne vlasti. Zajedno, zadatak institucija za nadzor obuhvata sve aspekte rada obavještajnih službi, uključujući njihovo poštivanje zakona; učinkovitost i efikasnost njihovih aktivnosti; njihove finansije; i njihove administrativne prakse.

Praksa 7. Nadzorne institucije imaju ovlast, sredstva i stručno znanje da pokreću i provode vlastite istrage, kao i puni i neometani pristup informacijama, zvaničnicima i objektima kako bi ispunile svoj mandat. Nadzorne institucije imaju punu saradnju obavještajnih službi i organa za provedbu zakona prilikom saslušanja svjedoka kao i pribavljanja dokumentacije i drugih dokaza.

Praksa 8. Nadzorne institucije preduzimaju sve potrebne mjere da zaštite klasificirane informacije i lične podatke kojima imaju pristup u toku svog rada. Utvrđene su kazne za kršenje ovih zahtjeva od strane predstavnika i nadzornih institucija.

5. PREPORUKE

- Učinkoviti sistemi nadzora koriste unutarnja i vanjska tijela – uključujući tu više rukovodstvo službe, izvršnu vlast, sudstvo, parlamentarne odbore, stručna tijela, institucije ombudsmena, glavne revizorske institucije, civilno društvo i medije.
- Mandati tijela koja čine sistem nadzora nad obavještajnim službama treba da obuhvate ispravnost, zakonitost, učinkovitost i efikasnost cijele obavještajne zajednice.
- Barem jedno tijelo u sistemu nadzora nad obavještajnim službama treba da bude civilno, nezavisno i vanjsko u odnosu na obavještajne službe i izvršnu vlast.
- Šta tačno predstavlja obavještajnu službu, treba definirati na jedan funkcionalan način. Tačnije, svaka državna organizacija čiji je primarni zadatak prikupljanje, analiza i diseminacija nacionalnih sigurnosnih informacija je obavještajna služba.
- Monitoring aktivnosti službe treba da obuhvati puni ciklus nadzora nad obavještajnom službom kojeg čini prethodni - ex ante, tekući i naknadni - ex post nadzor.
- Učinkovitost sistema nadzora nad obavještajnim službama trebaju redovno ocjenjivati nezavisna tijela.
- Tijela za nadzor nad obavještajnim službama treba redovno da komuniciraju sa sličnim institucijama iz inostranstva kako bi identificirali i razmijenili dobre prakse.

Bilješke

1. Ovaj priručnik koristi termin *obavještajna služba, a ne obavještajna agencija ili obavještajno tijelo*, kako bi se naglasilo da te organizacije obavljaju javnu službu.
2. Organizacija za ekonomsku saradnju i razvoj, *OECD DAC Handbook on Security System Reform: Supporting Security and Justice* (Paris: OECD, 2007), str. 140.
3. Za informacije o privatnim firmama, vidjeti Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York: Simon & Schuster, 2008).
4. Za potpuniju diskusiju o tome šta znači odgovornost javne agencije, vidjeti Mark Bovens, "Public Accountability," u *The Oxford Handbook of Public Management*, ured.i Ewan Ferlie, Laurence E. Lynne Jr, I Christopher Pollitt (Oxford: Oxford University Press, 2005).
5. Vijeće Evrope, Evropska komisija za demokratiju putem prava (Venecijanska komisija), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), Stav 73.
6. Na primjer, vidjeti Ronnie Kasrils, "To spy or not to spy? Intelligence and democracy in South Africa," u *To spy or not to spy? Intelligence and democracy in South Africa*, ured. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), str. 9¬–20.
7. Na primjer, vidjeti SAD, Ministarstvo odbrane, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," Direktiva br. 5148.11, 21. maj 2004.
8. Bugarska, Zakon o državnoj agenciji za nacionalnu sigurnost, 44. sjednica Narodne skupštine, Čl. 88.
9. Bosna i Hercegovina, Zakon o obavještajnoj i sigurnosnoj agenciji, 22. mart 2004, Čl. 42.
10. Južna Afrika, Ministarska komisija za praćenje rada obavještajnih službi, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10. septembar 2008), str. 77.
11. U Holandiji, ministarska odgovornost je bila ugrađena u Ustav već 1848; vidjeti A. D. *Belinfante, Beginselen van Nederlands Staatsrecht*[Principles of Dutch Constitutional Law] (Alphen aan de Rijn: Samson Publishers, 1981), str. 64–66.
12. Christian Heyer, "Parliamentary Oversight of Intelligence: The German Approach," u *Intelligence and Human Rights in the Era of Global Terrorism*, ured. Steve Tsang (Westport, CT: Praeger Security International, 2007), str. 69.
13. Vijeće Evrope, Evropska komisija za demokratiju putem prava (Venecijanska komisija), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), stav 78.
14. Istražna komisija vezana za određene aktivnosti Kraljevske kanadske konjičke policije (McDonald Commission), *First Report: Security and Information* (9. oktobar 1979), str. 425.
15. Neke države koriste hibridnu formu nadzornog tijela čiji članovi uključuju i nezavisne stručnjake i bivše članove parlamenta.
16. Vidjeti, Ujedinjeno Kraljevstvo, Obavještajni i sigurnosni odbor, *Godišnji izvještaj za 2001–2002*, CM 5542 (2002), str. 46–50.
17. Za detaljnije informacije, vidjeti Australija, Inspector-General of Intelligence and Security Act 1986, Zakon br. 101 iz 1986. Kako je dopunjen; i website Generalnog inspektora za obavještane i sigurnosne službe (dostupno na http://www.igis.gov.au/).
18. Ian Leigh, "National courts and international intelligence cooperation," u *International intelligence cooperation and accountability*, ured.i Hans Born, Ian Leigh, i Aidan Wills (London: Routledge, 2011), str. 232.
19. Frederic Manget, "Another system of oversight: intelligence and the rise of judicial intervention," u *Strategic intelligence: A window into a secret world*, ured.i Loch Johnson i James Wirtz (Los Angeles: Roxbury, 2004), str. 407–409.
20. Ian Leigh, "National courts and international intelligence cooperation," in I*nternational intelligence cooperation and accountability*, eds. Hans Born, Ian Leigh, and Aidan Wills (London: Routledge, 2011), str. 232.
21. Holandija, Zakon od 7. februara 2002, kojim se utvrđuju pravila vezana za obavještajne i sigurnosne službe i izmjene i dopune nekoliko zakona (Intelligence and Security Services Act 2002), Čl. 83, stav 1, str. 31.
22. Ibid., Čl. 84, stav 1, str. 31.
23. Dana Priest i William M. Arkin, "Top Secret America: A Washington Post Investigation," *The Washington Post, four-part article series*, July–December 2010 (dostupno na: http://projects.washingtonpost.com/top-secret-america/; pristup ostvaren 18. novembra 2011).
24. Holandija, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report: 2010–2011*, str. 8–9.
25. Norveška, Zakon vezan za praćenje obavještajnih, nadzornih i sigurnosnih službi, Zakon br. 7 od 3. februara 1995, Čl. 2.
26. Ibid., Čl. 2.
27. Ibid., Čl. 8, stav 2.
28. Komisija za istragu djelovanja kanadskih zvaničnika u vezi sa Maherom Ararom, *A New Review*

Mechanism for the RCMP's National Security Activities (2006), str. 17.

29. Ibid., str. 17.
30. Mada se žalbe najčešće tiču događaja koji su se već desili, vrijedi zapaziti da se ponekad tiču i operacija koje su u toku ili, pak, nikad nisu izašle izfaze planiranja.
31. Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays*, ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995).
32. Cyrille Fijnaut, *Het Toezicht op de Inlichtingen- en Veiligheidsdiensten: de noodzaak van krachtiger samenspel* [Nadzior nad sigurnosnim i obavještajnim službama: poreba za tješnjom saradnjom] Hag, april 2012)(na holandskom).
33. United Nations Human Rights Council, *Report Of The Special Rapporteur On The Promotion And Protection Of Human Rights And Fundamental Freedoms While Countering Terrorism: Compilation Of Good Practices On Legal And Institutional Frameworks And Measures That Ensure Respect For Human Rights By Intelligence Agencies While Countering Terrorism, Including On Their Oversight*, United Nations Document A/HRC/14/46 (17. maj 2010).

POGLAVLJE 2

Uspostava učinkovitog sistema nadzora nad obavještajnim službama

Stuart Farson

DVA

2

Uspostava učinkovitog sistema nadzora nad obavještajnim službama

Stuart Farson

1. UVOD

Ovo poglavlje razmatra jednu od najvažnijih tema reforme sektora sigurnosti: uspostavu učinkovitog nadzora nad obavještajnim službama i mehanizama odgovornosti (posebno zakonodavnih mehanizama) u zemljama u tranziciji. Pitanje koje se odmah nameće je sljedeće: da li su mehanizmi koje koriste razvijene demokratije odgovarajući model za države koje su još uvijek u procesu uvođenja i unapređenja demokratskog načina upravljanja? Odgovor ovisi o karakteristikama konkretne države u tranziciji, uz uvažavanje relevantnih aspekata, kao na primjer kakva su očekivanja u smislu zadataka koje će vršiti te službe, koliki je zahvata njihovih aktivnosti, kao i sa kojim prijetnjama se države suočavaju u svom okruženju. Kod analize ovih faktora moraju se uzeti u obzir i šira pitanja, a posebno stepen razvoja demokratske političke kulture i stepen razvoja demokratske prakse u razmatranoj državi.

Stavljanje institucija vlasti pod demokratsku kontrolu i pozivanje na njihovu odgovornost jedan je od najznačajnijih zadaka demokratije. Međutim, demokratske države se međusobno razlikuju po načinu na koji to postižu. Neke se oslanjaju na parlamente da pozivaju vladu na odgovornost, dok je u drugima sistem više složen i isprepleten, te podrazumijeva postojanje i više različitih ekspertnih tijela. Učinkovitost ovog procesa, koji se uobičajeno naziva nadzor, ovisi ne samo o ovlaštenjima koja proistječu iz zakonskih i ustavnih odredbi koje određuju šta može biti predmet detaljnog nadzora, te gdje, kada i

koliko često je moguće nadzirati, već i o mjeri u kojoj su informacije dostupne tijelima za nadzor. Bez mogućnosti da stekne znanje i očuva svoje institucionalno sjećanje, niti jedno tijelo za nadzor ne može razviti stručnost koja mu je potrebna da bi znalo šta posmatrati i koja pitanja postavljati da bi ostvarilo svoje ciljeve.

Neovisne institucije, poput Ženevskog centra za demokratsku kontrolu nad oružanim snagama (Geneva Centre for the Democratic Control of Armed Forces) puno toga su postigle posljednjih godina na razvoju pravnih standarda i najboljih praksi za reformu sektora sigurnosti, posebno kad se radi o nadzoru nad obavještajnim službama.[1] U isto vrijeme su naučni radnici, osim što su istraživali pojedina nadzorna tijela, pokušali dati analizu funkcija obavještajnih službi i nadzora sa komparativnog stanovišta.[2] Ipak, vidan je nedostatak studija koje nastoje utvrditi longitudinalnu učinkovitost različitih modela nadzora nad obavještajnim službama.[3] U tom pogledu, objavljene su samo studije koje pokrivaju primjere iz Velike Britanije i SAD.[4]

Mali broj studija učinkovitosti različitih sistema nadzora predstavljaju ograničavajući faktor prilikom preporučivanja jedne institucije za nadzor u odnosu neku drugu. Prvo, proučavanja sistema nadzora koja ne uključuju longitudinalnu evaluaciju imaju ograničenu komparativnu vrijednost (vrijednost koju sadrže leži ponajprije u problemima koje otkrivaju u modelima nadzora koje proučavaju). Drugo, sistemi nadzora UK i SAD koji su longitudinalno proučavani možda ne predstavljaju najbolje modele za zemlje u tranziciji. U slučaju Sjedinjenih Država, na primjer, obim i dimenzije njihovog obavještajnog aparata, veliki budžeti i mjera u kojoj je uključen privatni sektor u obavještajnu zajednicu čine proučavanja nadzora nad obavještajnim službama SAD-a nečim što je tek od skromne vrijednosti za zemlje u tranziciji, gdje su okolnosti bitno drugačije.

Ukazujući na razlike između različitih oblika demokratskog upravljanja, sljedeći dio ovog poglavlja razmatra osobenosti zemalja u tranziciji. Treći dio se bavi karakteristikama učinkovitog nadzora. Četvrti dio identificira nekoliko institucionalnih pristupa nadzoru koji su razvijeni u različitim državama, posvećujući pažnju njihovim prednostima i manama. Peti dio nudi analizu prepreka za učinkovit nadzor, dok se šesti dio bavi pravnim ovlastima koje nadzorna tijela moraju imati da bi mogla funkcionirati. Na kraju ovog poglavlja je dato nekoliko ključnih preporuka..

2. DRŽAVE U TRANZICIJI

Države koje se nalaze u procesu razvoja demokratskih načina upravljanja često se nazivaju „države u tranziciji“. Sve one dijele zajedničko iskustvo demokratizacije, ali po svemu ostalom imaju malo sličnosti, i razlikuju se ne samo po svojim polaznim tačkama, nego i po obliku demokratije za koju su se opredijelile. Neke od njih su nekada bile demokratske zemlje, prije nego što su prošle kroz totalitarnu fazu. Neke su, pak, novoosnovane države koje su nastale nakon raspada veće države, dok su neke prošle kroz duboke etničke podjele, ili čak građanski rat. Dijelom u ovisnosti o njihovoj posebnoj historiji, pravac u kojemu se razvijaju njihove demokratije se također razlikuje. Neke stvaraju unitarnu državu, dok druge razvijaju federalnu. Neke uspostavljaju predsjednički sistem sa jasnom podjelom vlasti i definiranim mehanizmima kočnice i ravnoteže u izvršnoj vlasti. Druge se, pak, odlučuju za parlamentarni sistem koji objedinjuje zakonodavnu i izvršnu granu vlasti. Neke su ustavne monarhije, a druge su republike. Neke imaju izborni sistem „relativne većine“ (eng. „first-past-the-post“), a druge jedan od oblika proporcionalne zastupljenosti. Neke

imaju jednodomno zakonodavno tijelo, a druge dvodomno. Osim toga, razlikuju se i njihovi pravosudni sistemi. Sve u svemu, izbor koji svaka zemlja u tranziciji napravi ima izravan utjecaj na vrstu političke kulture koju razvija.

Politička kultura neke demokratske države, posebno mjera u kojoj javnost prihvaća demokratske vrijednosti, određuje način na koji će se te vrijednosti zaživjeti u praksi. Članovi izvršne vlasti jedne države će, na primjer, spremnije prihvatiti javnost svoga djelovanja nego pripadnici izvršne vlasti druge države. Stoga će se, također, i razvoj zakonodavne odgovornosti razlikovati od države do države. Ono što negativno utječe na ovaj napredak u pravcu demokratskog upravljanja u dosta slučajeva je pokret ka de-demokratizaciji[5] – kojeg podstiče sveprisutna sklonost onih koji su na vlasti da (zlo)upotrebljavaju instrumente države kako bi očuvali svoju vlast, i, posebno, korupcija.

Čak se i terminologija demokratskog upravljanja može razlikovati od jedne zemlje do druge, posebno kad se koristi u specifičnom kontekstu nadzora nad obavještajnim službama. *Odgovornost (polaganje računa)* se, na primjer, generalno smatra procesom podnošenja rezultata, izvještaja, ili tumačeno slobodnije, implicira transparentnost. Ipak, u državama Commonwealtha koje slijede vestminsterski model demokratije, ovaj vid odgovornosti podrazumijeva i konkretnu ustavnu obavezu od strane nadležnih ministarstava da pruži istinite izvještaje u parlamentu i za parlament o svim djelovanjima (ili propuštanjima djelovanja) organizacija koje su u njihovoj nadležnosti. Drugi termini koji mogu imati promjenjivo značenje su, između ostalog: *prijetnje, rizici, nacionalna sigurnost, neovisnost, diskrecija, kompetencije, sigurnost, obavještajne službe* kao i sam *nadzor*.

3. UČINKOVIT NADZOR

Svaki zakonodavac, prije nego što uspostavi sistem nadzora nad obavještajnim radom, treba prosuditi izglede da taj sistem bude učinkovit. S obzirom koliko je putno literature na ovu temu sada dostupno moglo bi se pomisliti da se radi o lakom zadatku. Međutim, ovdje je potrebno izreći par napomena. Iako je nekoliko naučnih radnika nedavno objavilo veoma korisne studije u kojima opisuju djelovanje pojedinih nadzornih tijela, vrlo malo njih se bavilo učinkovitošću tih tijela na način koji bi bio dovoljno detaljan i koji bi obuhvatao dovoljno dugi vremenski period da bi se mogli izvući pouzdani zaključci. (Nažalost, studije koje se odnose na dovoljno dugi vremenski period nisu razvile korisne kriterije za prosudbu učinkovitosti.)

Ono što dodatno otežava je činjenica da izvršna i zakonodavna vlasti često imaju različite ciljeve nadzora. Kao rezultat toga, mnoge demokratske zemlje su razvile jedan mješoviti sistem u kojemu više nadzornih tijela ispunjavaju različite svrhe i pokrivaju različite oblasti nadzora. U takvom sistemu, parlamentarni odbori mogu postojati zajedno sa stručnim nadzornim tijelima, i nekada djelovati koordinirano, a nekada ne.

Kakav god da je uspostavljeni sistem, važno je da zakonodavna vlast bude informirana o aktivnostima nadzornih tijela, da od njih dobija pravovremene informacije i da izvještaji tih tijela budu lako dostupni – što često nije uvijek bio slučaj. Ono što je posebno važno jeste da zakonodavac mora uvijek biti svjestan zadatka koji se želi ostvariti kroz obavještajni nadzor. U suprotnom, nadzor može postati više simbolični nego istinski.[6] Možda bi se moglo reći da je cilj jednostavan i da je isti za svaku vladinu agenciju. Cilj nije da se kontrolira rad obavještajnih službi[7] već da se od njih i od izvršne vlasti traži odgovornost

i polaganje računa zakonodavnoj vlasti za njihovo djelovanje odnosno nedjelovanje, na način koji javnost može vidjeti i shvatiti. Uvažavajući izrečeno, ipak, određeni elementi kontrole mogu nastati kao posljedica barem dvije od najvažnijih nadležnosti parlamenta da razmatra i potom odobrava korištenje javnih sredstava za pokrivanje troškova aktivnosti obavještajnih službi i da usvaja odnosno vrši izmjene zakonodavstva koje regulira rad tih službi.

Pri izvršavanju obaveze nadzora, zakonodavac treba procijeniti svoje sposobnosti, sklonosti i ograničenja. Nedostatak vremena, ograničen nivo stručnosti i nedostatni resursi svakako utječu na rezultate koji se realno mogu postići. Prema tome, zakonodavac treba dobro razmisliti o tome što želi postići i na koji način se to može ostvariti unutar parlamentarnog radnog ciklusa. Možda bi stručno nadzorno tijelo bilo pogodnije za određene zadatke nadzora. Ako je tako, kakav će biti odnos parlamenta prema tom tijelu?

Vrlo grubo rečeno, parlamenti se trebaju baviti nadzorom nad obavještajnim službama na dva određena načina: jedan se odnosi na usklađenost, a drugi na efikasnost. Tačnije, parlamenti se trebaju pobrinuti da obavještajne službe i oni sa kojima oni sklapaju ugovore ne krše zakon, i pravila službe odnosno politike vlade. Također, trebaju se pobrinuti da se javna sredstva koriste pravilno i učinkovito.

Ipak, prečesto se dešava da članovi parlamenta pretpostave da je njihova osnovna odgovornost da vrše ex post ocjenu (reviziju) djelovanja obavještajnih službi – to jest, da naknadno detaljno preispitaju što se dešavalo. Ovo je samo djelomično ispravno. Iako je veliki dio pažljivog praćenja moguć tek nakon što se nešto desi, članovi parlamenta ipak imaju odgovornost da vrše nadzor obavještajne aktivnosti prije i tokom njene realizacije. Na primjer, članovi parlamenta su nadležni da osiguraju da postoje potrebna pravila i politike vlade prije nego što se ostvare operacije. Isto tako, iako se efikasnost može prosuđivati tek naknadno, sposobnosti i kriteriji performansi se trebaju procijeniti unaprijed i na tekućoj osnovi.

4. PRISTUPI NADZORU

U ovom dijelu analiziraju se tri pristupa nadzoru koja se trenutno koriste u nizu demokratskih država. To su, redom:

- pristup kongresnih i parlamentarnih odbora;
- pristup generalnog inspektora;
- pristup stručnih nadzornih tijela.

Ovdje je termin *zakonodavni odbor* korišten generički i obuhvaća ne samo parlamentarne odbore nego i odbore zakonodavnih tijela koje se ne smatraju parlamentima.

4.1 KONGRESNI I PARLAMENTARNI ODBORI

Odbori koji postoje u zakonodavnim tijelima se razlikuju po vrsti i kapacitetima. U nekim zemljama, kao što su one koje primjenjuju vestminsterski model demokratije, odbori mogu odražavati neku mjeru fuzije ili preklapanja između izabranih članova zakonodavnog tijela i izvršnog dijela vlade. U drugim zemljama, opet, ne postoji nikakvo preklapanje.[8]

Na samom početku je potrebno istaći značajnu razliku između odbora koji postoje u predsjedničkom sistemu i onih koji se nalaze kod parlamentarnih demokratija. Ovdje je od najvećeg značaja razlika u pristupu odgovornosti. U Sjedinjenim Državama, gdje stroga podjela ovlasti potiče svaku granu vlasti da kontrolira one druge, sam Kongres ima moć da odlučuje koje će informacije dobivati i koja će pitanja razmatrati kroz svjedočenje na svojim odborima. Ovlaštenja za raspodjelu javnih sredstava i usvajanje zakona, koje su date isključivo Kongresu, osiguravaju da, sa znakovitim izuzecima, će se ovo ispoštovati. Stoga kongresni odbori SAD-a redovno saslušavaju svjedočenja cijelog niza viših zvaničnika izvršne vlasti, uključujući i šefove obavještajnih službi od kojih se očekuje da pruže potpune odgovore na pitanja koja se odnose na politiku i upravljanje. (Izabrani predstavnici izvršne vlasti SAD-a – to jest, predsjednik i potpredsjednik – ne svjedoče pred Kongresom.

Nasuprot tome, u većini parlamentarnih sistema, izvršna vlast ima zadnju riječ u tome da li će se neka povjerljiva informacija dostaviti odborima, čisto zato što stranka koja ima vlast po definiciji kontrolira parlamentarnu većinu. Također, postoji i primjetna razlika u očekivanjima koja se odnose na to ko će se pojaviti na ovim odborima i na koje teme će se odnositi pitanja. U nekim parlamentima, izabrani predstavnici izvršne vlasti se pojavljuju pred odborom da odgovaraju na pitanja vezana za politiku, dok se drugi izvršni zvaničnici pojavljuju po svom nahođenju i govore o upravljačkim i administrativnim pitanjima.

4.1.1 Kongresni pristup u Sjedinjenim Državama i Brazilu

U Sjedinjenim Državama, kao posljedica istraga Odbora Churcha i Pikea iz 1970-ih, Kongres je odlučio uspostaviti stalne odbore za obavještajne službe i u Predstavničkom domu i u Senatu. Ovi odbori su imali zadatak da pažljivo prate djelatnosti obavještajnih službi SAD-a, i obraćaju pažnju istovremeno na ispravnost i na efikasnost njihovog rada. Ovi odbori se sastaju na sigurnim lokacijama i podržava ih veliki broj osoblja koje je prošlo sigurnosne provjere, i imaju ovlasti da vrše prethodni, tekući i naknadni nadzor. Odgovornost za pažljivo praćenje rada domaćih obavještajnih službi u SAD-u sad je također i na kongresnim odborima koji nadziru rad Ministarstva pravde (Justice Department) i Ministarstva domovinske sigurnosti (Department of Homeland Security). Osoblje odbora, koje imenuju i većinske i manjinske stranke, pruža pomoć predstavnicima svojih stranaka. Osim njih, mogu se koristiti i usluge važnih agencija za podršku rada Kongresa, kao što je Kongresna služba za istraživanje (Congessional Research Service) i Vladin ured za odgovornost (Government Accountability Office).

Brazil je još jedan primjer kongresnog sistema, koji je nedavno napustio vojnu vladavinu i prešao na demokratiju i federalno uređenje. Tokom barem jedne decenije nakon tranzicije iz 1985. godine, nova izvršna vlast Brazila je uglavnom posvećivala pažnju rješavanju hitnih problema, kao što je ekonomija i ogroman vanjski dug zemlje. Ove preokupacije, zajedno sa raširenom percepcijom da Brazil nema vanjskih neprijatelja, doveli su do toga da reforma obavještajnog sektora nije smatrana kao hitna.[9] Međutim, odnedavno je brazilski Kongres ne samo otpočeo ovu reformu, nego je uspostavio i niz kongresnih odbora čiji je cilj da vrše kontrolu obavještajnih službi. Tako je 1999. godine uspostavljeno ono što se danas naziva Zajedničkom komisijom za kontrolu obavještajnih aktivnosti (Joint Commission for the Control of Intelligence Activities ili CCAI). Potom su uspostavljene još četiri kongresne komisije: komisije za odbranu i u Predstavničkom domu i u Senatu, Komisija za javnu sigurnost protiv organiziranog kriminala u Predstavničkom domu i stalna Podkomisija Komisije Senata za javnu sigurnost, ustav, pravosuđe i državljanstvo. Sve one su bile uspješne u postizanju višeg nivoa transparentnosti – mada je CCAI u prvim

godinama nakon svog osnivanja trpjela negativne posljedice male zainteresiranosti među članovima Kongresa, nemogućnosti da postigne sporazum o internim pravilima komisije i nedovoljnih tehničkih resursa i pomoćnog osoblja.[10]

4.1.2 Parlamentarni pristupi

Parlamentarni pristupi nadzoru nad obavještajnim radom razlikuju se ne samo od kongresnog pristupa, nego se razlikuju i između sebe.[11] Ključna se razlika odnosi na pristup povjerljivim informacijama, ljudskim i drugim resursima koji im stoje na raspolaganju, mandat odbora i način imenovanja njegovih članova.

Postoji najmanje pet pristupa nadzoru nad obavještajnim službama koje trenutno primjenjuju parlamenti:

- parlamentarni odbori bez prava pristupa povjerljivim podacima;
- zakonom ustanovljeni odbori sastavljeni od članova parlamenta;
- stalni zakonom ustanovljeni parlamentarni odbori;
- posebni zakonom ustanovljeni odbori za ocjenu;
- mješoviti odbori i sistemi.

Parlamentarni odbori bez prava pristupa povjerljivim podacima

U pojedinim parlamentarnim demokratijama (poput Kanade ili Irske), izvršna vlast ne predviđa posebna pravila za pristup parlamentarnih odbora povjerljivim informacijama. Prema tome, svaka osoba unutar kruga povjerljivosti – to jest, koja je prošla provjere za rad sa povjerljivim informacijama – bi vjerojatno činila krivično djelo ukoliko bi „procurila“ takvu informaciju nekom članu parlamenta. Kao rezultat toga, parlamentarni odbori u tim demokratijama moraju djelovati bez bilo kakvog „insajderskog“ poznavanja obavještajnih poslova. A ipak, oni nisu sasvim nemoćni. Pošto ipak raspolažu punim istražiteljskim ovlastima i resursima parlamenta, mogu vršiti korisne ocjene i skrenuti vladi pažnju na neka važna pitanja.[12]

Ovdje je važno istaći još dvije važne napomene u vezi sa ovim pristupom. Najprije, sigurno je da postoje neka pitanja koja se ne mogu adekvatno pokriti. Na primjer, kada stručna nadzornih tijela istaknu konkretne probleme koji podstiču zabrinutost, parlament se ne može tako lako upozoriti na njih. Drugo, u nedostatku utvrđenog mandata, izbor pokrivenih pitanja će biti dosta nesistematičan. Osobe na čelu odbora se mijenjaju, pa će se tako mijenjati i njihov plan rada, prakse i institucionalno sjećanje.

Zakonom ustanovljeni odbori sastavljeni od članova parlamenta

Drugi pristup, prisutan u Ujedinjenom Kraljevstvu, oslanja se na zakonom uspostavljene odbore parlamentarnih zastupnika.[13] Uspostavljeni zakonom, a ne voljom parlamenta, Odbor za obavještajnu službu i sigurnost UK (Intelligence and Security Committee ili ISC) je sastavljen od članova Donjeg doma (House of Commons) i Gornjeg doma (House of Lords) koji su izabrani ne od strane političkih stranaka, kao što je slučaj sa parlamentarnim odborima, već od strane premijera, kojemu ISC podnosi izvještaje. Razlog za ovo rješenje je što ISC nije pravi parlamentarni odbor. Na primjer, on ne raspolaže istražnim ovlastima parlamentarnog odbora i ne može koristiti uobičajene parlamentarne resurse i privilegije. Umjesto toga, radi se o odboru parlamentarnih zastupnika.

Najvažnija prednost ovakvog odbora je što ima pristup povjerljivim podacima, sastaje se u sigurnom okruženju i ima osoblje koje je prošlo sigurnosne provjere. Još jedna njegova prednost je kontinuitet. Članovi odbora koji dolaze iz Gornjeg doma ne treba, za razliku od kolega iz Donjeg doma, tražiti reizbor, te je stoga moguće ostvariti snažniji kontinuitet i razvoj institucionalnog sjećanja.

Sa druge strane, zakonom utvrđen mandat ISC-a je ograničen, i obuhvaća samo rashode, administrativna pitanja i politike glavnih obavještajnih službi. Također su ograničeni i njegovi istražni resursi. Iako je nedavno situacija donekle unaprijeđena, ona još nije na poželjnom nivou. Kao posljedica toga, ovaj pristup uglavnom ne potiče kontinuirano praćenje dešavanja, što bi se moglo smatrati važnim aspektom nadzora.

Napori da se ISC podvede pod parlamentarnu kontrolu su do sada bili bez uspjeha, ali je uloga političkih stranaka porasla. One sada ostvaruju snažan utjecaj na izbor članova ISC-a i vrijeme parlamenta za diskusiju o prečišćenim (javnim) verzijama izvještaja ISC-a redovno se planira.[14]

Stalni zakonom ustanovljeni parlamentarni odbori

Stalni zakonom ustanovljeni parlamentarni odbori za obavještajnu djelatnost razlikuju se od prethodnog pristupa po tome što se ovdje radi o pravim parlamentarnim odborima. Njihove članove imenuju političke stranke, i oni mogu po potrebi koristiti resurse parlamenta.

Za razliku od ISC-a, čiji zaposlenici služe izvršnoj vlasti, stalni parlamentarni odbor može u velikoj mjeri sam određivati pravce djelovanja, ne samo u smislu koje osoblje će zaposliti (pod uvjetom da su prošli sigurnosnu provjeru), nego i gdje će se sastajati (pod uslovom da se radi o sigurnoj lokaciji).

Uslovi za članstvo se razlikuju od zemlje do zemlje. U Južnoj Africi, na primjer, proporcionalna zastupljenost je pravilo, pa sve važne političke stranke moraju biti zastupljene u odboru. Na Novom Zelandu, s druge strane, i premijer i lider opozicije moraju biti članovi ovog Odbora. U Australiji, odbor mora okupljati članove iz oba doma saveznog parlamenta.

Zakoni koji uspostavljaju ove stalne parlamentarne odbore obično definiraju i koje organizacije podliježu njihovom preispitivanju. Iako se ponekad izostavljaju određene aktivnosti, i ono što ostane može biti dosta široko. U Australiji, na primjer, Zajednički parlamentarni odbor za obavještajni rad i sigurnost (Parliamentary Joint Committee on Intelligence and Security ili PJCIS) ima mandat da pažljivo prati rad najvažnijih obavještajnih organizacija u zemlji, iako je i lista aktivnosti koje ne podliježu razmatranju ovog odbora također dosta duga (vidjeti Okvir 1).

Okvir 1: Ograničenja mandata australskog Zajedničkog parlamentarnog odbora za obavještajni rad i sigurnost

Djelovanje Odbora se ne odnosi na:

a. ocjenu prikupljanja obavještajnih informacija i procjenu prioriteta Australijske organizacije za sigurnosno-obavještajni rad (Australian Security Intelligence Organisation - ASIO), Australijske tajne obavještajno-sigurnosne službe (Australian Secret Intelligence Service - ASIS), Organizacije za obrambeno geo-prostorno snimanje (Defence Imagery and Geospatial Organisation - DIGO), Organizaciju za odbrambeni obavještajni rad (Defence Intelligence Organisation - DIO), Direkciju za odbrambenu signalizaciju (Defence Signals Directorate - DSD) i Ured za nacionalnu procjenu (Office of National Assessments -ONA);
b. uvid u izvore informacija, drugu operativnu pomoć ili operativne metode koji su na raspolaganju ASIO-u, ASIS-u, DIGO-u, DIO-u, DSD-u ili ONA-i;
c. uvid u određene operacije koje su poduzete, u toku su ili se predlaže njihovo poduzimanje od strane ASIO, ASIS, DIGO, DIO ili DSD;
d. uvid u informacije koje se dobivaju od strane vlade, ili, pak, posredstvom neke od njenih agencija, a ukoliko ta vlada ne pristane na objelodanjivanje informacije;
e. uvid u neki aspekt djelovanja ASIO, ASIS, DIGO, DIO, DSD odnosno ONA koji se ne odnosi na državljane Australije;
f. razmatranje pravila koja su usvojena u skladu sa Čl. 15. ovog Zakona;
g. vođenje istraga o pojedinačnim žalbama koje se odnose na djelovanje ASIO, ASIS, DIGO DIO, DSD ili ONA;
h. razmatranje sadržaja ili zaključka koji su sadržani u izvještaju ili procjenama koje su napravile DIO ili ONA, niti uvid u izvore informacija na kojima se zasnivaju te procjene odnosno izvještaji;
i. uvid u aktivnosti koordinacije i evaluacije koje poduzima ONA.[15]

Značajna razlika između ovog i prethodnog pristupa pravnih odbora parlamentarnih zastupnika i stalnih pravnih parlamentarnih odbora je u ovlastima i privilegijama koje odbori imaju. Stalni zakonom ustanovljeni odbori mogu optužiti za nesaradnju strane koje ne ispoštuju zahtjeve odbora, a posebno se to odnosi na izradu dokumentacije i evidencije. Osim toga, australijski zakon izričito naglašava da svaki dom parlamenta može uputiti „bilo koje pitanje“ koje se odnosi na najvažnije službe na razmatranje PJCIS-u.[16]

Posebni zakonom ustanovljeni odbori za nadzor

U barem jednoj državi (Kanada) budući članovi parlamenta su zakonom obavezani da uspostave odbore čiji je zadatak da pažljivo prate primjenu zakona o obavještajnim službama kada ti zakoni budu na snazi nekoliko godina. Usvajanjem kanadskog Zakona o obavještajnoj službi (Canadian Security Intelligence Service Act) i Zakona o sigurnosnim prekršajima (Security Offenses Act) 1984. godine izričito je naloženo parlamentu da uspostavi odbor koji će razmatrati primjenu tih zakona nakon što budu na snazi pet godina.[17] Kanadski Zakon o borbi protiv terorizma (Anti-Terrosim Act) usvojen 2001. godine isto tako obavezuje parlament da uspostavi odbor za ocjenu nakon tri godine.[18] U svakom od navedenih slučajeva, mandat odbora bio je da razmotri odredbe i primjenu zakona i da u svoj izvještaj uključi preporuke za sve izmjene koje smatra potrebnima.

Ovi odbori, čija je priroda bila *ad hoc*, imali su fiksno trajanje od jedne godine, po čijemu isteku su podnosili izvještaj. S obzirom da nisu bili viđeni kao sastavni dio sigurnosnog

kluba, uživali su malu pomoć stručnih nadzornih tijela koja su također uspostavljena tim zakonima.[19]

Mješoviti odbori i sistemi

Jedan broj zemalja uspostavilo je mješovite odbore u čijem su sastavu i članovi zakonodavnog tijela i pojedinci koji nisu članovi ni izvršne ni zakonodavne vlasti.

Švedska Komisija za zaštitu sigurnosti i integriteta
U Švedskoj, na primjer, predsjedavajući i zamjenik predsjedavajućeg Komisije za zaštitu sigurnosti i integriteta (SAKINT) mora imati iskustvo sudije ili ekvivalentno pravničko iskustvo. Preostali članovi odbora, kojih može biti najviše deset, imenuju se na osnovu nominacije stranačkih grupa u švedskom parlamentu (Riksdag), koji mogu ali ne moraju biti aktualni članovi parlamenta.

SAKINT ima dvije najvažnije odgovornosti: da nadzire primjenu tajnog nadzora, prikrivenih isljednika, kao i druge specijalne istražne radnje koje koriste agencije za borbu protiv kriminala; i da nadzire obradu osobnih podataka od strane Švedske sigurnosne službe. SAKINT ispunjava svoje nadležnosti uglavnom kroz inspekcije čija je svrha da osigura poštovanje zakona i propisa Švedske.

Pri vršenju svoje djelatnosti SAKINT uživa podršku osoblja kojemu je na čelu direktor imenovan od strane vlade. Zakon kojim je uspostavljen SAKINT daje ovlasti ovom odboru da dobija informacije i koristi pomoć tijela koja su predmet njegovog nadzora. SAKINT podnosi godišnje izvještaje vladi. Takva obaveza ne postoji prema Riksdagu.

Mješoviti sistem u Njemačkoj
U Njemačkoj, sistem nadzora nad obavještajnim službama je kombiniran na sličan način. Neki ga nazivaju „multilateralnim“ jer ga čini više tijela koja djeluju paralelno.[20] Najvažnije tijelo je Parlamentarni kontrolni panel (PKG), stalni panel za nadzor nad obavještajnim službama donjeg doma njemačkog parlamenta (Bundestaga). Po zakonu, PKG se mora sastajati barem jednom u svakom kvartalu. Iako članstvo u PKG-u odražava stranački sastav Bundestaga, na poziciji predsjedavajućeg se na godišnjoj osnovi smjenjuju pripadnik parlamentarne većine i pripadnik opozicije. Članovi ovog odbora uživaju pomoć sedmočlanog sekretarijata. Fokusiraju se na aktivnosti tri savezne obavještajne službe i razmatraju pitanja *in camera* (iza zatvorenih vrata). Odbor može pozvati radnike obavještajne službe da svjedoče, mogu po potrebi dobiti dokumente i ući u prostorije službe u bilo kojem trenutku. Ovaj odbor svoje izvještaje mora podnijeti Bundestagu u sredini i na kraju svakog izbornog termina.

Drugo tijelo je Povjerljivi odbor (Confidential Committee) koji je odgovoran za pažljivo praćenje budžeta obavještajni službi (riječ je o ukupnim iznosima koji se dostavljaju Odboru za budžet Bundestaga za uključivanje u prijedlog budžeta). Značajno je spomenuti da PKG i Povjerljivi odbor ponekad održavaju zajedničke sastanke kada se razmatraju budžetska pitanja. (vidjeti Poglavlje 8 – Wills koja sadrži dodatne informacije).

Posljednja komponenta njemačkog mješovitog sistema je Komisija G10 – neovisno, kvazisudsko tijelo čije su odluke obavezujuće za obavještajnu službu i vladu. Četiri člana Komisije G10, koje bira PKG, mogu biti članovi Bundestaga, ali i to nije obavezno.

Komisija G10 je prvobitno bila osnovana kako bi ovlastila i nadzirala presretanje pošte i telekomunikacija koje vrše obavještajne službe. Međutim kada su amandmani na zakon o borbi protiv terorizma iz 2007. godine predvidjeli davanje novih ovlaštenja obavještajnim službama, uloga Komisije G10 se također promijenila. Sada Komisija G10 izdaje odobrenja obavještajnim službama za pristup zadržanim podacima telekomunikacijskih operatera, kao što su na primjer lokacija sa koje se telefonira, serijski broj ili šifra kartice.

4.2 GENERALNI INSPEKTORI

U ovom dijelu razmatraju se tri različita pristupa zakonskoj uspostavi institucije Generalnih inspektora (GI).[21] Prvi, koji je uspostavljen u Sjedinjenim Državama, poslužio je kao model za duga dva pristupa. Pored toga, oni se međusobno bitno razlikuju po tome ko postavlja GI, kome GI podnosi izvještaj i na koje se teme ti izvještaji odnose. Praktična iskustva pojedinih GI se također razlikuju, jer neki imaju veću mogućnost pristupa ključnom osoblju i informacijama od drugih.

4.2.1 Generalni Inspektor Centralne obavještajne agencije Sjedinjenih Država

Iako je Zakonom o generalnom inspektoru iz 1978. godine propisano da svi važniji odjeli vlade SAD-a imaju svoje Generalne inspektore, to se nije odnosilo na Centralnu obavještajnu agenciju (Central Intelligence Agency – CIA), koja je već od ranije imala svog posebnog GI. Uspostavljen 1952, GI za CIA-u je 1978. godine još uvijek imenovao direktor agencije i, po mišljenju mnogih, on nije uživao dovoljnu neovisnost. Tek 1989. godine je GI-CIA konačno zakonom uređen, te je dobio veću neovisnost. GI-CIA je i dalje zaposlenik CIA-e i podnosi izvještaje direktoru, ali sada ovaj položaj zauzima osoba koju nominira predsjednik a potvrđuje Senat, i može je smijeniti samo predsjednik.

Uloga GI-CIA je prije svega da promovira ekonomičnost, učinkovitost i efikasnost, kao i odgovornost unutar CIA-e. On/ona to čini tako što vrši neovisne revizije, inspekcije, istrage i procjene programa i operacija CIA-e. GI-CIA je također nadležan za otkrivanje i odvraćanje od prevara, neopravdanog trošenja resursa, zloupotrebe i nepravilnosti u upravljanju. Što se tiče izvještavanja, od GI-CIA se zahtijeva da svoje nalaze i preporuke blagovremeno prenese direktoru Agencije, kao i kongresnom obavještajnom odboru. Kada se nalazi odnose na navodne povrede zakona, GI-CIA mora također obavijestiti državnog pravobranitelja (Attorney General).[22]

4.2.2 Generalni inspektor Sigurnosno-obavještajne službe Kanade

Za razliku od GI za CIA-u, koji je zaposlenik agencije koju nadzire, osoba koja vrši dužnost Generalnog inspektora Obavještajno-sigurnosne službe Kanade (Office of the Inspector General of the Canadian Security Intelligence Service ili OIG-CSIS) nije zaposlen u toj službi nego u Ministarstvu javne sigurnosti (Ministry of Public Safety), a imenuje ga kabinet i izvještaje podnosi Zamjeniku ministra za javnu sigurnost. Mandat OIG CSIS-a, koji je određen Zakonom o obavještajno-sigurnosnoj službi Kanade (Canadian Security Intelligence Service Act) iz 1984. godine, je mnogo slabiji nego što je to mandat IG-CIA. OIG CSIS se fokusira u potpunosti na pridržavanje zakona, propisa i politika Kanade. Svakih dvanaest mjeseci, ovo tijelo mora razmotriti izvještaj koji podnosi direktno CSIS nadležnom ministru koji se odnosi na operativne aktivnosti službe. OIG-CSIS ima zadatak da potvrdi izvještaj, ukazujući na sve aktivnosti koje nisu u skladu sa Zakonom o CSIS-u, ili koje su u suprotnosti sa uputama koje izdaje ministar. Osim toga, OIG-CSIS mora identificirati sve aktivnosti koje predstavljaju neopravdano ili nepotrebno korištenja ovlasti CSIS-a.

Zakon posebno daje pravo OIG-CSIS-u da od direktora CSIS-a i drugi zaposlenika CSIS-a traži sve informacije, izvještaje i objašnjenja koja smatra potrebnim za vršenje svojih dužnosti. U praksi, međutim, GI ima problema da se sastane sa direktorom CSIS-a.

OIG-CSIS ne komunicira izravno sa parlamentom, čak ni kada se radi o pitanjima nepoštivanja zakona. U stvari, parlamentarni predstavnici mogu doći do ovih saznanja na samo tri načina: ako nadležni ministar dobrovoljno odluči da ih informira; ako dođu do informacije na osnovu zahtjeva u skladu sa Zakonom o pristupu informacijama; ili ako je informacija uključena u jedan od godišnjih izvještaja koje priprema Odbor za nadzor sigurnosno-obavještajnih službi (Security Intelligence Review Committee – SIRC), stručno tijelo koje djeluje izvan izvršne vlasti (vidjeti Dio 4.3. dalje u tekstu).[23]

4.2.3 Generalni inspektor za obavještajno-sigurnosne službe Australije

Generalni inspektor za obavještajno-sigurnosnu službu i sigurnost Australije (Australian Inspector General of Intelligence and Security – AIGIS), slično kao i institucija iz Kanade, utemeljen je zakonom. Osnovan 1986. godine Zakonom o generalnom inspektoru za obavještajne službe i sigurnost (Inspector General of Intelligence and Security Act), ovaj ured nije dio niti jednog ministarstva ili agencije. Umjesto toga, predstavlja neovisno tijelo koje je u okviru portfelja premijera.

AIGIS, kojega imenuje glavni guverner, ima mnogo šire polje djelovanja nego GI SAD-a ili Kanade. Umjesto da pažljivo prati samo jednu službu, on ili ona je odgovoran za cjelokupno obavještajnu djelatnost Australije. Iako AIGIS u određenoj mjeri obavlja različite funkcije prema različitim službama, njegove/njene najvažnije dužnosti su trostruke:

1. praćenje usklađenosti za zakonima, uputama i smjernicama koje reguliraju aktivnosti pojedinih službi;
2. procjena ispravnosti tih aktivnosti;
3. procjena učinkovitosti tih aktivnosti;
4. utvrđivanje da li neka od tih aktivnosti nije u skladu ili krši ljudska prava.

Možda i ne iznenađuje što je AIGIS historijski najveći dio svojih istražnih resursa fokusirala na Sigurnosno-obavještajnu organizaciju Australije (Australian Security Intelligence Organisation - ASIO). Razlog za to je što je nadležnost ASIO prvenstveno domaća, pa je stoga veća vjerovatnost da će ugrožavati prava državljana i stanovnika Australije nego službe koje rade u inostranstvu i odbrambene obavještajne službe Australije. (Nedavno izvršene procjene govore da se od 60 do 70 posto resursa AGIS-a troši na programe proaktivne inspekcije.[24]) Kada vrši punu istragu, AIGIS može koristiti i koristi ista istražna ovlaštenja koja inače imaju kraljevske istražne komisije. To znači da AIGIS može zahtijevati da se svjedoci pojave na saslušanju i da istinito svjedoče. Također, ima ovlasti i zahtijevati dostavu dokumenata i stupiti u prostorije službe. U međuvremenu, neovisnost i stalnost mandata AIGIS-a postignut je činjenicom da se može smijeniti samo ako postoji opravdan razlog za sijenu.

AIGIS je Zakonom obavezana da podnosi godišnji izvještaj o svojim aktivnostima Premijeru, koji ga mora staviti na dnevni red oba doma parlamenta. Iako bivši vršitelji ove dužnosti smatraju da je AIGIS tijelo za nadzor koje ne može naložiti promjene,[25] preporuke tog ureda obavještajne službe i nadležni ministri ipak uzimaju vrlo ozbiljno.[26]

I na kraju, treba spomenuti da, osim što su pod nadzorom AIGIS-a i PJCIS-a (koji se razmatra gore u tekstu), obavještajne službe Australije su također pod pažljivim okom Nacionalnog ureda za reviziju Australije (Australian National Audit Office).

4.3 STRUČNA NADZORNA TIJELA

Stručna nadzorna tijela se obično uspostavljaju zakonom. Njihove posebne karakteristike se odnose na funkciju koju obavljaju, stepen neovisnosti od izvršne vlasti i parlamenta, kojem podnose izvještaj, način izbora njihovih članova, te po tome da li postoje neki posebni uslovi za članstvo.

4.3.1 Kanadski Odbor za ocjenu rada sigurnosno-obavještajnih službi i Ured povjerenika za sigurnost komunikacija

Kanada ima dva takva stručna nadzorna tijela: SIRC (Odbor za ocjenu rada sigurnosno-obavještajnih službi ili izvorno *Security Intelligence Review Committee*) i Ured povjerenika za sigurnost komunikacija Kanade (izvorno *Office of the Communications Security Establishment Commissioner Canada* odnosno OCSEC). SIRC, koji djeluje izvan kako izvršne tako i zakonodavne vlasti, ima najviše pet članova koji moraju biti povjerljivi savjetnici (eng. privy councillors) i prema tome pod zakletvom povjerljivosti. Osim toga, niti jedan član SIRC-a ne smije biti aktualni član parlamenta.[27] Izvorno, ideja je bila da će članovi biti osobe sa iskustvom povjerljivih savjetnika koje su stekli na funkciji nadležnih ministara. Ali ovo nije uvijek bio slučaj. SIRC se sastaje na sigurnim mjestima i ima pomoć osoblja koje je prošlo sigurnosne provjere. Osim što dobije sigurnosni certifikat OIG-CSIS-a, SIRC ima i vlastiti mandat da osigura poštivanje zakona CSIS-a, koji uključuje i ovlasti da vrši istrage pritužbi na ovu službu (vidjeti Okvir 2). U tom pogledu, može dati upute OIG-CSIS-u ili samoj službi da izvrši ocjenu određenih aktivnosti.

Okvir 2: Mandat Odbora za ocjenu sigurnosno-obavještajnih službi Kanade

Funkcije Odbora za ocjenu su:

a. da vrši generalnu ocjenu vršenja dužnosti i funkcija Službe, i u vezi s tim:
   i. da razmatra izvještaje direktora i potvrde generalnog inspektora koje mu se dostavljaju u skladu sa potčlanom 33(3);
   ii. da razmatra upute koje izdaje ministar u skladu sa potčlanom 6(2);
   iii. da razmatra aranžmane koje sklapa Služba u skladu sa potčlanovima 13(2) i (3), kao i 17(1) , i da prati pružanje informacija i obavještajnih informacija u skladu sa tim aranžmanima;
   iv. da pregleda sve izvještaje i komentare koje mu se dostavljaju u skladu sa pod-članom 20(4);
   v. da prati sve zahtjeve navedene u stavu 16(3) koji su upućeni Službi;
   vi. da pregleda propise, i
   vii. da prikuplja i analizira statističke podatke vezane za operativne aktivnosti Službe;
b. da organizira vršenje procjene, odnosno dâ ocjenu u skladu sa Čl. 40, i
c. da vrši istrage u vezi sa.
   i. (i) žalbama dostavljenim Odboru u skladu sa Čl. 41. i 42;
   ii. (ii) izvještajima dostavljenim Odboru u skladu sa Čl. 19. Zakona o državljanstvu (Citizenship Act); i
   iii. (iii) pitanja koja su upućena Odboru u skladu sa Čl. 45. Zakona o ljudskim pravima Kanade (Canadian Human Rights Act).[28]

Pri obavljanju ovih ocjena SIRC ima pravo pristupa svim informacijama koje su pod kontrolom OIG-CSIS-a ili CSIS-a, koje SIRC smatra potrebnim za vršenje svojih dužnosti i funkcija – uključujući izvještaje i objašnjenja. SIRC može podnositi izvještaje nadležnom ministru po svom nahođenju. Međutim, uvijek mora podnositi godišnji izvještaj kojega nadležni ministar može staviti na dnevni red parlamenta. Iako SIRC može određivati sadržaj izvještaja, u njemu ne smiju biti sadržane povjerljive informacije.

Izvorno se očekivalo da će godišnji izvještaj SIRC-a pružati parlamentu informacije koje su mu potrebne da vrši učinkovit nadzor nad obavještajnim službama. U praksi, međutim, SIRC nije uvijek bio tako predusretljiv.[29]

Kada se Specijalni odbor donjeg doma parlamenta za ocjenu Zakona o CSIS-u i Zakona o sigurnosnim prekršajima (vidjeti Dio 4.1.2.4 gore u tekstu) sastao da razmatra odgovarajuće uloge SIRC-a i OIG-CSIS-a, njegovi članovi nisu mogli shvatiti zašto se funkcije OIG-CSIS-a ne bi mogle unijeti u funkcije SIRC-a. Tadašnji resorni ministar se morao snažno boriti da uvjeri specijalni odbor u važnost OIG-CSIS-a i potrebu istovremenog postojanja oba ova tijela. Kao posljedica toga, specijalni odbor je promijenio kurs i suzdržao se od davanja preporuke da se raspusti OIG-CSIS. Međutim, nakon nekoliko godina, sljedeća vlada je prihvatila ostavku dotadašnjeg čelnog čovjeka ove institucije, a posljedica toga je da je to mjesto ostalo upražnjeno više od godinu dana. Tek vrlo skoro je vlada ukazala da sada namjerava integrirati OIG-CSIS u SIRC. Iako je ova odluka opravdana potrebom za smanjenjem administrativnih troškova, istovremeno je istaknuto da treba unaprijediti nadzor.[30]

Do 1996. godine, kada je izvršnom uredbom osnovan OCSEC, Organizacija za sigurnost komunikacija (Communications Security Establishment - CSE), Obavještajna služba Kanade za presretanje komunikacija (Canada's signals intelligence service) nije bila obuhvaćena vanjskim nadzorom. Pet godina kasnije, u okviru omnibus Krivičnog zakona, parlament je usvojio Zakon o borbi protiv terorizma, koji je pružio zakonsku osnovu za rad i OCSEC-u i CSE, koji su do tada,djelovali na osnovu izvršne uredbe. Zakon o borbi protiv terorizma dao je OCSEC-u ograničeni mandat da osigura da CSE radi u skladu sa zakonima Kanade. OCSEC je također ovlašten da saslušava pritužbe na rad agencije. Uslovi koje osoba treba ispunjavati da bi bila postavljena na ovu funkciju su, između ostalog, iskustvo višeg sudije. Nakon što stupi na funkciju, osoba se iz OCSEC-a može smijeniti samo ako postoji opravdan razlog.

Poput OIG-CSIS-a i SIRC-a, OCSEC funkcionira u okviru kruga povjerljivosti, sa osiguranim prostorijama i ograničenim osobljem koje je prošlo sigurnosne provjere. Osim toga, OCSEC ima iste istražiteljske ovlasti kao i svaki drugi povjerenik u skladu sa Zakonom o istragama. Poput SIRC-a OCSEC ima obavezu podnositi godišnji izvještaj koji će resorni ministar staviti na dnevni red parlamenta.

Ova dva godišnja izvještaja su jedini izvor informacija koje kanadski parlament dobiva izravno od OCSEC-a i SIRC-a. Ni u jednom slučaju vlada nije obavezna poduzeti aktivnosti na osnovu preporuka izvještaja.

4.3.2 Belgijski Stalni odbor za ocjenu rada obavještajnih agencija

Jedno stručno tijelo slično SIRC-u vrši nadzor nad obavještajnim službama u Belgiji. Ipak, Belgijski stalni odbor za ocjenu rada obavještajnih agencija (*Belgian Standing Intelligence*

Agencies Review Committee) poznat pod nazivom Odbor I, razlikuje se od kanadskog primjera u nekoliko važnih aspekata. Prvo, njegov mandat obuhvaća dvije obavještajne službe: Državnu sigurnost) koja je civilna služba i Opću obavještajno-sigurnosnu službu, koja predstavlja vojni pandan Državnoj sigurnosti, kao i Koordinacijsku jedinicu za procjenu prijetnji.[31] Drugo, mandat Odbora I ide dalje od osiguranja pridržavanja zakona i propisa,te zalazi u razmatranje efikasnosti rada službi i koordinacije između njih. Treće, tri člana Odbora I – od kojih svi moraju proći sigurnosne provjere, imati diplomu pravnika, kao i relevantno profesionalno iskustvo – imenuje Senat Belgije (a ne, kao što je slučaj u Kanadi, kabinet). I na kraju, predsjedavajući odbora mora biti sudija.

Niti jedan član Odbora I ne može biti član parlamenta, ali zakon koji uspostavlja odbor obavezuje oba doma parlamenta da uspostave stalne odbore koji će pratiti rad Odbora I i razmatrati njegove izvještaje. Zakon, dalje, predviđa da članovi parlamentarnih odbora poduzmu odgovarajuće sigurnosno mjere i nameće im obavezu da čuvaju povjerljivost informacija koje im se povjere, čak i nakon što napuste funkciju, ili će u suprotnom biti krivično gonjeni.

5. PREPREKE UČINKOVITOM NADZORU

U zemljama u tranziciji postoji veliki broj činioca koji mogu ometati uspostavu učinkovitog nadzora. U ovom dijelu razmatraju se prepreke koje se najčešće javljaju u nadzoru nad obavještajnim službama.

5.1 NEVOLJNOST DA SE IZVRŠNA VLAST POZIVA NA ODGOVORNOST

Najosnovnija prepreka učinkovitom nadzoru jeste nevoljnost zakonodavca da usvoji i primijeni mjere kojima pozivaju izvršnu vlast da položi račune za svoje djelovanje. U zemljama u tranziciji, gdje izvršna vlast nije ranije pozivana na odgovornost, zakonodavci obično moraju eksperimentirati sa više pristupa prije nego što utvrde koji je za njih najbolji. Oslanjati se samo na rasprave u odboru u očekivanju da pruže učinkovit nadzor vjerojatno će se pokazati nedovoljnim. Iskustvo pokazuje da je angažiranje pomoćnog osoblja, istraživačke studije, studijska putovanja i saslušanja iza zatvorenih vrata (*in camera*) također potrebni.

5.2 STRMA KRIVULJA UČENJA

Sigurnosne i obavještajne aktivnosti se razlikuju od većine dugih funkcija vlade po tome što utječu i/ili uključuju gotovo sve odjele odnosno ministarstva. Pošto pravilan nadzor iziskuje veliki stepen upoznatosti sa funkcijama i praksama obavještajnih službi i kompleksnim načinima na koji oni ostvaruju međudjelovanje sa drugim vladinim agencijama, krivulja učenja je strma i stoga stavlja zakonodavce u težak položaj jer osim prethodnih imaju i mnogobrojne druge zahtjeve kojima moraju posvetiti vrijeme i pažnju. Razvoj potrebne stručnosti iziskuje vrijeme, posebno kada se uzme u obzir generalna nevoljnost ljudi koji rade u obavještajnim službama da podijele svoje konkretno znanje.

5.3 NEDOSTATAK POVJERENJA

Ako obavještajne službe i tijela za njihov nadzor ne vjeruju jedni drugima, neće biti otvorene diskusije, niti značajnih razmjena informacija, te neće biti moguće vršiti učinkovit

nadzor. Da bi se izgradio odnos povjerenja, vanjska nadzorna tijela (posebno kongresni i parlamentarni odbori) trebaju izbjegavati isključivu fokusiranost na poštivanje zakona. Takvo ograničavanje nadzora bi moglo dovesti do toga da nastane konfrontacija, odnos mi-protiv-njih, što bi obeshrabrilo radnike obavještajnih službi da prepoznaju bilo kakvu korist od procesa nadzora. Umjesto toga, barem u početnoj fazi, oni vide samo velike teškoće.

Da bi nadzor bio učinkovit i obavještajne službe trebaju osjetiti koristi od njega. Naglasak na efikasnost, na primjer, može biti od koristi službi tako što će se dati preporuke koje će potaći izvršnu vlast da za službu izdvoji veća sredstva. Služba također može iskusiti korist od nadzora kada neki odbor zakonodavnog tijela ili stručno nadzorno tijelo ispravi neki izvještaj u medijima koji neopravdano optužuje radnike službe za nezakonito djelovanje ili dovodi u pitanje njihovu učinkovitost.

5.4 USKRAĆIVANJE PRISTUPA OSOBAMA, MJESTIMA, DOKUMENTACIJI I EVIDENCIJI

Pojedinačno najvažnija prepreka učinkovitom nadzoru jeste uskraćivanje pristupa osobama, mjestima, dokumentaciji i evidenciji. Bez ovog pristupa nadzornih tijela ne mogu adekvatno funkcionirati (vidjeti, također, Nathan – Poglavlje 3). Ona ne mogu provjeriti da li je informacija koju su dobili od izvršne vlasti tačna, niti mogu pravilno sprovesti istrage nekog konkretnog pitanja. Umjesto toga, moraju se oslanjati isključivo na ono što im se kaže i što mogu dobiti iz otvorenih izvora.

5.5 PRITISAK KRATKIH ROKOVA I NJIHOV UTJECAJ NA NADZOR

Pritisak kratkih rokova koje se pred zakonodavce nameće može imati negativan utjecaj na izbor adekvatne vrste nadzora koji će preduzeti. Studije kongresnih nadzornih odbora SAD-a su pokazale da su veći izgledi da će se zakonodavci, umjesto da sami otkrivaju probleme, baviti pitanjima koja su već privukla pažnju javnosti[32]. A za to imaju dobre razloge. Naime, pošto su zakonodavci zauzeti ljudi sa velikim brojem obaveza (među kojima je svakako i nastojanje da budu ponovno izabrani), često se bave onim pitanjima koja im potencijalno mogu donijeti najveću političku korist. Činjenica da se pažljivo praćenje obavještajnih službi rijetko dešava u javnosti znači da im nudi malo mogućnosti da ostvare političku korist.

Kapaciteti zakonodavaca da nadziru obavještajne službe su dodatno ograničeni samom prirodom zakonodavne vlasti. Vrijeme koje je na raspolaganje za nadzor je ograničeno ne samo zbog poslova koje svi zakonodavci moraju obaviti, nego i rasporedom zasjedanja zakonodavnog tijela. U većini jurisdikcija, zakonodavni rad se obustavlja kada zakonodavno tijelo ne zasjeda, kao i tokom izbora. Prenošenje odgovornosti za nadzor na neko stručno tijelo nudi djelomično rješenje za ovaj problem.

5.6 STRANAČKA PRISTRASNOST

Proces nadzora lako može ugroziti stranačka pristrasnost. U Sjedinjenim Državama, na primjer, pretjerana stranačka pristranost može onemogućiti napore opozicije da ostvari detaljan uvid u rad obavještajnih službi tako što se odlaže ili kontrolira rad kongresnih odbora za nadzor.[33] Isto tako, kako u najvećem broju parlamenta vladajuća stranka ima većinsku zastupljenost, ona kontrolira dnevni red odbora zakonodavnih tijela. Da bi se suprotstavilo ovakvoj dominaciji, koja je opće pravilo, u nekim parlamentima je obavezno

da predsjedavajući odbora za nadzor nad obavještajnim službama bude član opozicione stranke.

Ovakav izbor predsjedavajućeg i izbor članova odbora zasnovanih na uspostavi pravilne ravnoteže između vlade i opozicije su važni načini na koje se može minimizirati stranačka pristranost i promovirati suradnja. Općenito govoreći, funkcije nadzora su najbolje kada članovi odbora za nadzor rade skupa u kolektivnom nastojanju da ostvare ciljeve od nacionalnog interesa.

5.7 KAŠNJENJE U PODNOŠENJU IZVJEŠTAJA STRUČNIH NADZORNIH TIJELA

U slučaju kada su stručna tijela ta koja obavljaju različite proaktivne i rutinske oblike nadzora, jako je važno da ona svoje izvještaje i analize dostavljaju parlamentu pravovremeno. Bez obzira koji aspekt obavještajnog rada podliježe detaljnom razmatranju od strane zakonodavaca, oni moraju biti svjesni što šire slike da bi obavljali tako široko postavljene zadatke kao što je raspodjela javnih sredstava i razmatranje postojeće legislative. Ako zakonodavci ne mogu dobiti izvještaje u pravo vrijeme i ne mogu pitati članove stručnih tijela o tome koje su njihove preporuke, mogućnost zakonodavca da odgovori svojim obavezama će biti ugrožena.

5.8 NEDOVOLJNI RESURSI

Mogućnost zakonodavca da vrši učinkovit nadzor zavisi u velikoj mjeri od resursa koji su im stavljeni na raspolaganje. Najvažniji resursi u tom smislu su osoblje i pristup. Kako je već ranije spomenuto, zakonodavci su zauzeti ljudi sa velikim rasponom obaveza. Bez pomoći stalnog, visoko stručnog i nestranačkog osoblja sa širokim poznavanjem obavještajnih krugova, zakonodavci će u najboljem slučaju vršiti ograničeni nadzor, svodeći svoje aktivnosti na saslušanja na odboru umjesto na istražni rad. Dalje, da bi mogli vršiti učinkovit nadzor, zakonodavcima je neophodno osigurati široki spektar informacija, uključujući zaključke istraživanja i sposobnosti vršenja revizije (eng. audit).

Stvaranje stalnog nestranačkog osoblja također može pomoći u razvoju i održavanju institucionalnog sjećanja. Pošto je potrebno dugo vremena da se razviju stručna znanja na polju obavještajnog rada, smjena zakonodavaca (koja može biti vrlo česta u pojedinim političkim sistemima) često dovodi do gubitka znanja i iskustva. Iz očiglednih razloga, postojanje stalnog, nestranačkog osoblja ublažava ovu smetnju učinkovitom nadzoru.

6. KREIRANJE PRAVNOG I INSTITUCIONALNOG OKVIRA ZA SISTEM NADZORA

Mandati nadzornih tijela treba da budu postavljeni na najširim mogućim osnovama. Iako mandat za neko konkretno tijelo za nadzor u velikoj mjeri zavisi od njegovog položaja u cjelokupnom sistemu nadzora, uzeti kao cjelina ovi mandati trebaju pokrivati široki spektar pitanja vezanih za rad obavještajnih službi, od administracije i operacija do politika i budžeta.

Da bi sistem nadzora bio učinkovit, mora postići da obavještajne službe koje prati poštuju odnosne zakone, propise i politike i da su učinkovite u ostvarivanju svojih zadataka. Iako

praćenje zakonitosti može biti relativno jednostavan zadatak, procjena učinkovitosti je mnogo kompleksnija jer iziskuje sveobuhvatno ispitivanje sigurnosno-obavještajnog sistema u cjelini. U tom nastojanju nije dovoljno samo pažljivo promatrati agencije koje prikupljaju obavještajne podatke. Također treba istražiti da li su izabrani nosioci vlasti: aktivno i rutinski angažirani na utvrđivanju strategija i nadležnosti za obavještajne službe, definiranju obavještajnih zahtjeva koji odgovaraju tekućim prijetnjama i mogućnostima,angažirani na utvrđivanju prioritete u radu službi i da li se staraju da se različiti dijelovi obavještajnog sistema pridržavaju tih prioriteta.

Ako se razmatra sigurnosni i obavještajni sistem u cjelini, čini se očiglednim da, ako se želi da bude koristan u zaštiti nacionalne sigurnosti, mora biti u stanju u svakom trenutku pružiti vladi „najbolju istinu“ do koje je moguće doći. Međutim, obavještajni rad nije savršena znanost i „najbolja istina“ može katkad imati ozbiljne mane, jer je takva priroda posla. U svakom slučaju, od velikog je značaja da obavještajne službe „govore istinu vlastima“ (eng. „speak truth to power”), bez obzira na posljedice neuspjeha. Da bi se ovakav stav promovirao i održao u obavještajnoj zajednici, službama treba puna podrška svih političkih stranaka, ali i pravična kritika. Problem je u tome što je parlament političko tijelo, gdje opozicione partije nastoje pokazati da su bolje od vladajuće stranke nudeći alternativna rješenja. Stoga iskušenje promoviranja partijskih interesa je često jače od spremnosti spremnost na saradnju, koje je na taj način ugroženo. Iz tog razloga je nadzor nad obavještajnim službama često najučinkovitiji kada ga provode stručna nadzorna tijela koja nisu izravno povezana niti sa izvršnom niti sa zakonodavnom vlašću. Ovakav aranžman nudi mogućnost da se nadzor nad stručnim službama zaštiti od političkih utjecaja.

Što se tiče zakonitosti rada obavještajnih službi, stručna nadzorna tijela trebaju imati mandat ne samo da vrše naknadnu ocjenu aktivnosti službe, nego i da razmatraju na tekućoj osnovi da li odnosni zakoni, propisi i politike dobro funkcioniraju ili ih treba mijenjati. Ova tijela također treba da imaju obavezu istraživanja pritužbi na rad službi koje imaju specijalne ili prinudne ovlasti, te treba da se staraju da nadležni organi do kraja istraže pritužbe (vidjeti Poglavlje 9 – Forcese). Pored toga, treba da budu obavezana da podnose redovne izvještaje svim relevantnim organima. Ti izvještaji, kada je to potrebno, treba da sadrže i preporuke za unapređenje problematičnih oblasti.

Što se tiče efikasnosti rada obavještajnih službi, stručna nadzorna tijela treba da mjere kako njihove kapacitete, tako i njihove učinke. Često se ovo mjerenje dešava naknadno (lekcije za ubuduće), ali svakako bi trebalo da postoji i tekuće mjerenje kojim se razmatra da li su trenutne sposobnosti službe odgovarajuće za ispunjenje budućih vladinih potreba. Institucije vrhovne revizije (eng. audit) obično raspolažu sposobnostima potrebnim da se razviju takva mjerenja (vidjeti Poglavlje 8 – Wills). Međutim, pošto su obično nadležne za cijeli niz vladinih aktivnosti, one ne mogu tokom redovnog obavljanja svojih dužnosti posvetiti dovoljnu pažnju obavještajnom sektoru. Kao posljedica toga, zakonodavna tijela mogu smatrati potrebnim da se vrhovnim institucijama za reviziju odobre posebni resursi ili da uspostave nova tijela za ovakvu reviziju koja će ispuniti ovu ulogu.

Kod definiranja mandata nadzornih tijela, zakonodavci se moraju pobrinuti da zakon pruži osobama koje rade u tijelima za nadzor pravo pristupa svim elementima bezbjednosne i obavještajne infrastrukture. Na taj način se omogućava tijelima za nadzor da procijene sveukupne sposobnosti obavještajne zajednice. Bez tako širokog polja djelovanja, izvršna vlast može i previše lako prebacivati odgovornosti kako bi izbjegla detaljni nadzor. Široko polje djelovanja također omogućuje osobama koje vrše nadzor da pažljivo razmotre

odnose između organizacija koji čine sastavni dio sistema, kako ti odnosi funkcioniraju u praksi te kako oni utječu na troškove zajedničkih operacija.

Nadalje, zakon kojim se osnivaju nadzorna tijela treba predvidjeti sigurnost funkcije za njegove članove kako bi se umanjio potencijalni utjecaj izvršne vlasti na njihove odluke. To znači da u organizacijskom smislu oni mogu biti pri izvršnoj vlasti, ali ne treba da budu unutar nje.

Dakle, moglo bi se postaviti pitanje, ako zakonodavac formira stručna tijela da vrše nadzor nad obavještajnim službama, kakav nadzor onda ostaje da ga vrše sami zakonodavci? Odgovor ima veze sa tri ključna zadatka koje zakonodavna tijela imaju u parlamentarnim demokratijama:

- da razmatra i usvaja pravne akte;
- da odobrava trošenje javnih sredstava ministarstva i organa (agencija) vlade;
- da zahtijeva od vlade odgovornost za svoje djelovanje odnosno nedjelovanje.

Sve ove odgovornosti podrazumijevaju da su parlamentarci aktivno uključeni u nadzor nad obavještajnim službama. Da bi ispunili svoje obaveze vezane za usvajanje zakona, budžeta i pozivanja na odgovornost, članovi odbora treba da imaju ne samo pravovremeni pristup izvještajima stručnih nadzornih tijela, nego i mogućnost da postave pitanja članovima tih tijela u vezi sa izvještajima koje su podnijeli. Osim toga, parlamentarci će katkad imati potrebu provesti vlastite istrage kada se pojave pitanja koja ugrožavaju povjerenje javnosti u obavještajne službe. Osim toga, oni će morati redovno pažljivo proučavati aktivnosti stručnih nadzornih tijela, kako bi se uvjerili da ona djeluju na učinkovit način i da raspolažu odgovarajućim resursima.

I na kraju, kako je već razmatrano u Dijelu 5.4, bez mogućnosti pristupa osobama, mjestima, dokumentaciji i evidenciji, ne može postojati učinkovit nadzor. Iz tog razloga najvažnija ovlast nadzornih tijela je pravo pristupa. Iako parlamentarci mogu imati opće pravo pristupa, odborima se ipak može uskratiti pristup povjerljivim informacijama, osoblju ili radnom okruženju, zato što uvjeti tog pristupa nisu jasno utvrđeni zakonom.

7. PREPORUKE

Zakoni koji uspostavljaju sistem nadzora nad obavještajnim službama bi trebali posebno obuhvatiti sljedeća pitanja:

Uspostava parlamentarnog odbora kojemu je odobren pristup osobama, mjestima, dokumentima i evidencijama.

Zakon koji omogućuje rad ovakvog odbora bi trebao specificirati njegove ovlasti u vezi sa pristupom – kao što je ovlaštenje da izdaje obavezujuće pozive, da zahtijeva svjedočenje ili iskaze pod zakletvom, te da ima pravo ulaska i pretraživanja prostorija obavještajne službe. Također treba definirati ko može postati članom ovog odbora i kojim resursima će odbor raspolagati. On treba da ima dva glavna zadatka, zakonom propisana, a to su: sprječavanje zloupotreba od strane sigurnosno-obavještajnih službi i unaprjeđenje učinkovitosti, efikasnosti i ekonomičnosti njihovog rada. Odbor bi, osim toga, trebalo da ima mogućnost davanja uputa svim tijelima za podršku da preuzmu aktivnosti nadzora

koje sâm nema kompetencija niti vremena vršiti, a te aktivnosti treba da se okončaju i o njima treba podnijeti izvještaj u razumnom vremenskom okviru.

Obaveze koje se stavljaju u nadležnost ovom odboru treba da uključuju zahtjev da se nadzor vrši u sigurnom okruženju. Njegovi članovi i osoblje treba da prođu sigurnosnu provjeru i treba da polože zakletvu da neće otkrivati povjerljive informacije.[34] Osim toga, iako može izdavati javne izvještaje kada smatra za shodnim, odbor bi trebalo obavezati da barem jednom godišnje podnese izvještaj koji će se naći na dnevnom redu parlamenta te će biti i objavljen. Svi ti izvještaji treba da prođu odgovarajuće provjere službi da slučajno ne sadrže neke povjerljive materijale, ali konačnu riječ u vezi sa temama koje će biti sastavni dio izvještaja ipak treba da ima odbor.

Dalje, zakon treba predvidjeti da odbor vrši redovne ocjene zakona koji se odnose na nacionalnu sigurnost kako bi utvrdio da li se zakon primjenjuje, te da li i dalje odražava postojeće prijetnje i tehnološko okruženje. Nadalje, zakon treba sadržavati konkretne kazne za članove odbora i osoblje odgovorne za „curenje“ informacija. I na kraju, treba predvidjeti ovlasti članova odbora da uspostave privremene, ad hoc istražne komisije kada se ukaže potreba za angažiranjem stručne osobe izvana, ili u vezi sa pitanjem koje će biti vrlo ispolitizirano.

Uspostava neovisnog tijela koje saslušava pritužbe na sve obavještajne službe.

Ovakvo tijelo bi trebalo biti prva tačka kontakta za sve koji se žale na neku obavještajnu službu. Zakon na osnovu kojeg se ovo tijelo osniva treba da predvidi posebnu zaštitu za tzv. „zviždače“, odnosno osobe koje upozoravaju na nepravilnosti u službi. Zviždače treba štititi samo pod uslovom da nisu otkrili povjerljive informacije koje nisu već ranije učinjene javnima, i da je to otkrivanje izvršeno u dobroj vjeri. Zaštita se treba primjenjivati i u slučajevima kada se naknadno prosudi da je otkrivanje bilo u javnom interesu. Štaviše, ovo tijelo bi trebalo također imati ovlasti da razmatra pojedinačne predmete nakon što je donesena presuda kako bi se utvrdilo da zviždači nisu trpjeli neprikladne posljedice vezane za svoje radno mjesto.

Uspostava jednog ili više nadzornih tijela koja nadzor vrše prvenstveno, ali ne isključivo, na vlastitu inicijativu.

Ova tijela treba da budu u mogućnosti da se slobodno sastaju i razgovaraju između sebe i sa parlamentarnim odborima, pod uvjetom da se susreti odvijaju u sigurnom okruženju. Također, oni mogu služiti potrebama izvršne vlasti, ali im primarna svrha treba biti pružanje pomoći parlamentarnim odborima u sprječavanju zloupotreba ovlaštenja i poticanje veće efikasnosti. Iako bi ova nadzorna tijela trebalo da imaju mogućnost izrade vlastitih planova i rasporeda rada, ona bi također trebalo da dobijaju smjernice od parlamentarnih odbora i izvršne vlasti. Oni mogu vršiti nadzor prije, tokom ili nakon događaja koje odluče preispitati.

Bilješke

1. Vidjeti, na primjer, Hans Born (uredn.), *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices* (Geneva: DCAF, 2003); kao i Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, i Parlament Norveške, 2005).
2. Komparativna razmatranja mogu se pogledati u Jean-Paul Brodeur, Peter Gill, and Dennis Tollborg (uredn.), *Democracy, Law, and Security: Internal Security Services in Contemporary Europe* (Aldershot, UK: Ashgate, 2003); Thomas C. Bruneau and Steven C. Boraz (uredn.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007); Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro (uredn.), *PSI Handbook of Global Security and Intelligence: National Approaches*, (Westport, CT: Praeger Security International, 2008); Greg Hannah, Kevin O'Brien, andAndrew Rathmell, *Intelligence and Security Legislation for Security Sector Reform*, Technical Report TR-288-SSDAT (RAND Europe, 2005).
3. Nekoliko studija se bavilo učinkovitošću određenih tijela za nadzor tokom određenog vremena. Među njima su: Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" u *Accountability for Criminal Justice: Selected Essays*, uredn. Philip C. Stenning (Toronto: University of Toronto Press, 1995), str. 185–212; Loch Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985); Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* (Chapel Hill: University of North Carolina, 1996); i Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (Maj 2007), str. 281–4.
4. Anthony Glees, Philip H.J. Davies, and John L. Morrison, *The Open Side of Secrecy: Britain's Intelligence and Security Committee* (London: Social Affairs Unit, 2006); Frank J. Smist Jr., *Congress OverVidis the United States Intelligence Community, 1947–1994, drugo izdanje* (Knoxville: University of TennesVidi Press, 1994).
5. Vidjeti Charles Tilly, *Democracy* (Cambridge: Cambridge University Press, 2007).
6. Vidjeti Peter Gill, "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984–88," *Intelligence and National Security* 4, br. 3 (1989) str. 550–575.
7. U parlamentarnim demokracijama, kontrola nad obavještajnim službama je obično u nadležnosti izvršne vlasti. Međutim, određeni elementi parlamentarne kontrole mogu nastati kao posljedica ovlasti parlamenata da odobravaju sredstva za djelovanje obavještajnih službi i usvajaju regulativu koje se one moraju pridržavati.
8. U određenim političkim sistemima gdje postoji podjela vlasti na grane, odbori zakonodavnih tjela ne mogu pozivati izabrane predstavnike izvršne vlasti da svjedoče.
9. Vidjeti Thomas C. Bruneau, "Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past," *Strategic Insights* VI, br. 3 (maj 2007.) (dostupno na http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485122).
10. Vidjeti Marco Cepik, "Structural Change and Democratic Control of Intelligence in Brazil," u Thomas C. Bruneau and Steven C. Boraz (uredn.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007) str. 149–169.
11. Za komparativnu analizu sistema parlamentarnog nadzora u Evropskoj uniji, pogledati Aidan Wills i Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (Brussels: European Parliament, 2011), posebno dijagrame na str. 92–95.
12. Kanadski Odbor Senata za nacionalnu sigurnost i odbranu pod predsjedničkim vodstvom Colina Kennyja obuhvatio je širok niz tema i napravio više važnih izvještaja, od kojih su neki zasnovani na radu in camera.
13. Kanada razmatra ovaj pristup, ali ga još nije usvojila.
14. Ovi izvještaji su prije rađeni u Kabinetu. Međutim, pošto postoji percepcija da bi potencijalno Kabinet mogao imati sukob interesa, sada se pripremaju u sigurnom okruženju koje se smatra više neovisnim.
15. Australija, Zakon o obavještajnim službama (Intelligence Services Act) 2001, Čl. 29(3).
16. Ibid., Čl. 29(1)(b).
17. Vidjeti Canada, Specijalni odbor za ocjenu Zakona o CSIS (CSIS Act) i Zakona o sigurnosnim prekršajima (Security Offenses Act), *In Flux But Not In Crisis* (septembar 1990).
18. Vidjeti Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (maj 2007), str. 281–4.
19. Vidjeti Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" u *Accountability for Criminal Justice: Selected Essays*, uredn. Philip C. Stenning (Toronto: University of Toronto Press, 1995), str. 185–212.

20. Vidjeti Shlomo Shpiro, "Parliamentary and Administrative Reforms u the Control of Intelligence Services in the European Union," *Columbia Journal of European Law* 4 (1998), str. 545–578.
21. Vidjeti Geoffrey R. Weller, "Comparing Western Inspectors General of Intelligence and Security," *International Journal of Intelligence and CounterIntelligence* 9, br. 4 (1996), str. 383–406.
22. Vidjeti Frederick M. Kaiser, "The watchers' watchdog: The CIA inspector general," International Journal of Intelligence and CounterIntelligence 3, No. 1 (1989), str. 55–75.
23. Tokom niza godina, kašnjenja u dobivanju sigurnosnih certifikata OIG-CSIS SIRC-a onemogućila su da ovaj odbor u godišnjem izvještaju razmatra – i tako obavijesti parlament – probleme u vezi sa poštovanjem zakona CSIS-a.
24. Vidjeti Ian Carnell and Neville Bryan, "Watching the Watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" (rad predstavljen na Konferenciji o zaštiti Australije (Safeguarding Australia Conference) 2005, 12–14 juli 2005) (dostupno na http://www.igis.gov.au/public_statments/conference_papers.cfm).
25. U pojedinim državama koje slijede Westminsterski model demokratije, članovi izvršne vlasti razlikuju ocjena (eng. review) i nadzora (eng. oversight). Termin *ocjena* koriste za čisto pažljivo praćenje, dok termin *nadzor* označava pažljivo praćenje i ocenu rada uz ovlasti da se uvedu promjene. Prema tome, kada pažljivo prate aktivnosti obavještajnih službi, tijela za ocjenu mogu dati samo preporuke poželjnih promjena, dok tijela za nadzor mogu nametnuti te promjene.
26. Vidjeti u Ian Carnell and Neville Bryan, "Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" (rad predstavljen na Konferenciji Sigurnost Australije (Safeguarding Australia Conference) 2005, 12–14. juli 2005) (dostupno na http://www.igis.gov.au/public_statments/conference_papers.cfm).
27. Izvorno je postojala nada da će članovi SIRC-a biti bivši nadležni ministri, ali to nije uvijek bio slučaj.
28. Kanadski Zakon o sigurnosno-obavještajnoj službi (Security Intelligence Service Act, R.S.C.), 1985, Poglavlje C-23, Čl. 38.
29. Vidjeti Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" u *Accountability for Criminal Justice: Selected Essays*, uredn. Philip C. Stenning (Toronto: University of Toronto, 1995), str. 185–212.
30. Bruce Cheadle, "Conservatives use budget bill to cut spy agency inspector general's office," *Canadian Press*, april 26, 2012.
31. Komitet I je također odgovoran da se pobrine da informacije o terorizmu i ekstremizmu Koordinacijska jedinica za procjenu prijetnje (Coordination Unit for Threat Assessment) proslijedi političkim administrativnim i sudskim vlastima.
32. Vidjeti, na primjer, Mathew D. McGubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms," *American Journal of Political Science* 28, br. 1 (februar 1984), str. 165–179.
33. Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 16, br. 1 (2003), str. 69–94.
34. Sigurnosna provjera (eng. veting) parlamentaraca i pojedinih drugih zvaničnika (poput sudaca) od strane sigurnosnih službi može biti neustavan sa stanovišta podele vlasti. To jest, općenito se smatra neprihvatljivim da netko iz izvršne vlasti odlučuje o podobnosti pripadnika zakonodavne ili sudske vlasti. Iz očiglednih razloga, ipak je potrebno provesti neki postupak sigurnosne provjere za sve one koji će svakodnevno raditi sa povjerljivim informacijama. Srećom, postoji više načina kako se može izbjeći naveden problem. Zakonodavna i sudska vlast mogu provesti vlastiti neformalni postupaksigurnosne provjere kakav se provodi kada se neka osoba imenuje na mjesto ministra. Također, mogu angažirati vanjsku sigurnosnu firmu da provede jedan formalniji postupak provjere. Ovako proveden postupak sigurnosne provjere postiže tri važna cilja. Prvo, sigurnosne službe će vjerojatnije imati više povjerenja i biti susretljivije kad se radi o nadzornim tijelima čiji su članovi prošli provjeru. Drugo, strani partneri će lakše podijeliti obavještajne informacije ako su uvjerene da te informacije tijela za nadzor neće dalje razotkrivati. Treće, proučavanja elita pokazuju da postoje „trule jabuke u svakom buretu". Suci su bivali korumpirani, članovi tijela za nadzor su bivali prinuđeni podnositi ostavke zbog sukoba interesa, pripadnicima zakonodavne vlasti utvrđivana je odgovornost za izdaju. Sigurnosna provjera može izdvojiti ove „trule jabuke" prije nego što one prouzrokuju štetu.

POGLAVLJE 3

Transparentnost, tajnost i nadzor nad obavještajnim službama

Laurie Nathan

3

Transparentnost, tajnost i nadzor nad obavještajnim službama

Laurie Nathan[1]

1. UVOD

Postojanje obavještajnih službi u demokratskim zemljama je u izvjesnom smislu politički paradoks. S jedne strane, ove službe se uspostavljaju da bi zaštitile državu, građane i druge osobe pod jurisdikcijom države, kao i demokratski poredak. U tu svrhu imaju posebna ovlaštenja i sposobnosti. Obično im zakon daje pravo da dolaze do povjerljivih informacija tajnim nadzorom, presretanjem komunikacija i na druge načine koji narušavaju pravo na privatnost; te da poduzimaju prikrivene operacije čiji je cilj suprotstavljanje prijetnjama po nacionalnu sigurnost; i da djeluju sa visokim nivoom tajnosti.

Sa druge strane, obavještajne službe i pripadnici izvršne vlasti mogu zloupotrijebiti te ovlasti i sposobnosti i time ugroziti sigurnost pojedinaca i narušiti demokratski proces. One mogu ograničavati ljudska prava protivno zakonu, ometati zakonite političke aktivnosti, te favorizirati ili imati predrasude prema nekoj političkoj stranci ili lideru. Mogu zastrašivati protivnike vlasti, stvoriti klimu straha i proizvoditi ili manipulirati obavještajnim podacima da bi ostvarili utjecaj na odluke koje vlada donosi, kao i na javno mišljenje. Također, mogu zloupotrebljavati sredstva i metode obavještajnih službi za ostvarivanje vlastite koristi.

S obzirom na ove opasnosti, demokratske zemlje su suočene sa izazovom uspostavljanja pravila, kontrola i mehanizama nadzora čiji je cilj smanjenje mogućnosti nezakonitog ponašanja i zloupotrebe ovlaštenja, te osiguranje da obavještajne službe ispunjavaju svoje dužnosti u skladu sa ustavom i zakonima.

Navedeno se jednako tako odnosi i na tijela za kontrolu i nadzor koja upravljaju drugim državnim organizacijama, ali te je ciljeve posebno teško ostvariti u svijetu obavještajnih službi zbog visokog nivoa tajnosti koja okružuje obavještajne službe i njihov rad. Tajnost ometa nadzor i ocjenu rada službi od strane nadzornih tijela, ograničava uvid javnosti u njihov rad i olakšava osobama koje rade u tim službama da prikriju nezakonitosti.

Ovo je poglavlje usmjereno na tajnost, transparentnost i davanje informacija nadzornim tijelima nad obavještajnim službama. Među tim tijelima su parlament, parlamentarni odbor za nadzor nad obavještajnim službama, pravosuđe, institucija vrhovne revizije, neovisni generalni inspektor za obavještajne službe (kao što je slučaj u Australiji, Novom Zelandu i Južnoj Africi) i stručno nadzorno tijelo (kao što je Odbor za ocjenu rada obavještajnih i sigurnosnih službi u Holandiji). Ovo poglavlje daje uvid u političku i konceptualnu debatu o tajnosti i transparentnosti obavještajnih službi, predstavlja dobre prakse vezane za zakone o zaštiti i pristupu informacijama i razmatra koje je obavještajne informacije potrebno dostaviti parlamentu i drugim tijelima za nadzor. U zaključku se nalazi skup preporuka.

Dok se razmatranja tajnosti obavještajnog rada općenito fokusiraju na to što se ne treba objaviti, ovo poglavlje na jedan pozitivniji način istražuje područja obavještajnog rada koja se moraju objaviti u interesu učinkovitog nadzora i demokratskog upravljanja.

Treba također naglasiti na samom početku da pretjerana tajnovitost dovodi do pojave sumnje i straha od obavještajnih organizacija, čime se smanjuje podrška javnosti za njih. U demokratiji, za razliku od policijske države, da bi bile uspješne obavještajne agencije se moraju oslanjati na saradnju sa javnosti, a ne na prinudu ili strah. Davanje više informacija o službi jača njihov profil na pozitivan način, smanjuje neugodnost i strah koje pokreće tajnovitost, unaprjeđuje saradnju sa službama i na taj način jača njihovu učinkovitost.

2. PROBLEM TRANSPARENTNOSTI I TAJNOSTI U NADZORU NAD OBAVJEŠTAJNIM SLUŽBAMA

Kada se radi o demokratskom upravljanju obavještajnim službama, najvažnije i ujedno najspornije pitanje je upravo pitanje tajnosti. Ono stvarno jeste najvažnije, jer što je veći nivo tajnosti, to je teže utvrditi i procijeniti karakteristike i rad službi. U nedostatku adekvatnih informacija, nadzornim tijelima je nemoguće utvrditi i smisleno raspravljati o ulozi i orijentaciji službi, potrebi za reformom obavještajnih službi, ili, pak, o vitalnom pitanju da li službe štite ili podrivaju sigurnost i slobodu građana i drugih osoba koje su pod jurisdikcijom države.

Ovo pitanje je veoma sporno jer ga karakteriziraju snažni suprotstavljeni interesi. S jedne strane, određeni aspekti obavještajne zajednice i njene aktivnosti se moraju smatrati tajnima da bi se izbjeglo ugrožavanje operacija i životi obavještajaca i njihovih izvora. S druge strane, tajnost za demokratsku vlast je anti-etična, jer sprječava punu odgovornost i predstavlja plodno tlo za zloupotrebu ovlaštenja, nezakonitost i kulturu nekažnjivosti.

Ovaj se odjeljak bavi debatama koje se odnose na transparentnost i tajnost obavještajnih službi i prikazuje demokratski pristup ovoj temi. Iskazana pitanja su od izuzetnog značaja za parlament. Pošto je uključen u izradu i usvajanje zakona i politika koje reguliraju tajnost i pristup informacijama, parlament ima značajnu ulogu u utvrđivanju mjere u kojoj je

vršenje obavještajnog rada otvoreno ili zatvoreno za pogled javnosti. Štoviše, parlament je ne samo odgovoran da poziva na odgovornost izvršne i državne organe, nego je i sam odgovoran prema javnosti i obavezan je pružiti građanima informacije o obavještajnoj zajednici. Rasprave u parlamentu o zakonima, politikama i budžetima koji se odnose na obavještajne službe se stoga trebaju odvijati na otvorenim zasjedanjima.

2.1 MOTIVI ZA TAJNOST OBAVJEŠTAJNIH SLUŽBI

Tajnost je jedna od osnovnih karakteristika obavještajnih službi zbog same prirode njihovog mandata i funkcije. Ove se službe bave konvencionalnim i nekonvencionalnim prijetnjama po nacionalnu sigurnost, neprijateljski nastrojenim zemljama i terorističkim i kriminalnim organizacijama, fizičkom zaštitom lidera iz vlade i državne uprave, te zaštitom tajnih državnih informacija. Tajnost daje obavještajnim službama konkurentnu prednost dok rade na navedenim pitanjima, a pretjerana transparentnost bi ih stavila u nepovoljan položaj i izrazito opasnu situaciju.

Konkretnije, svrhe tajnosti su slijedeće:

- spriječiti objekte obavještajnih operacija da postanu svjesni toga da su pod prismotrom;
- spriječiti objekte obavještajnih operacija i suparničke službe da saznaju o metodama koje službe koriste;
- zaštititi živote obavještajnih dužnosnika i doušnika;
- osigurati sigurnost vrlo važnih osoba (eng. VIP) koje su pod zaštitom obavještajnih službi;
- izbjeći na različite načine otkrivanje operacija od strane suparničkih obavještajnih službi.

Iako su ovi zahtjevi za tajnovitošću razumni, obavještajne službe su sklone tome da imaju pretjeran i katkad opsesivan stav prema tajnosti. Smatraju da će transparentnost u neosjetljivim područjima neizbježno dovesti do otvorenosti i u osjetljivim područjima, što će imati teške posljedice. Stoga razvijaju interne sisteme, procedure i pravila koja ne omogućuju nikakvo opuštanje ili fleksibilnost u vezi sa tajnošću. Također, činjenica je i to da ove službe cijene tajnovitost jer im daje određenu mističnost i elitni status.

Obavještajne službe katkad nevoljko otkrivaju informacije čak i parlamentarnim tijelima za nadzor koja su ovlaštena da dobivaju obavještajne podatke. Službe tvrde da, pošto zastupnici nisu obučeni i disciplinirani u smislu čuvanja povjerljivosti, postoji rizik da će osjetljive informacije otkriti neovlaštenim osobama ili zloupotrijebiti obavještajne podatke da bi postigli političku prednost za svoju stranku. Međutim, kako se navodi dalje u tekstu, može se primijeniti niz mjera za smanjenje rizika od neovlaštenog razotkrivanja informacija.

2.2 TAJNOST KAO IZUZETAK, A NE PRAVILO

Pošto su gore navedeni motivi za tajnost obavještajnih službi logični, mnogi radovi o demokratskom upravljanju obavještajnim službama ističu da se „mora postići odgovarajuća ravnoteža između tajnosti i transparentnosti“. Međutim, ovakva formulacija je previše neobavezujuća da bi bila od velike vrijednosti, i ne kreće sa pravog mjesta. Polazište bi trebalo naći među temeljnim postavkama demokratije. Među te postavke spada

transparentnost i pravo ljudi da ostvare pristup informacijama koje posjeduje država. One su od kritičnog značaja jer su preduslov za odgovornost izvršne vlasti prema parlamentu i nadzornim tijelima, učinkoviti nadzor tih tijela, političku i ličnu slobodu, demokratsko osporavanje vlasti, zdravu debatu i razmjenu ideja, puno korištenje prava građanstva i sprječavanje zloupotrebe vlasti.

Ideja da je sloboda informiranja osnova za druga prava i slobode izražena je u Rezoluciji Generalne skupštine Ujedinjenih Nacija 59(1) iz 1946. godine koja proglašava da je „sloboda informiranja temeljno ljudsko pravo i predstavlja mjerilo svih drugih sloboda kojima su posvećene Ujedinjene nacije". Ista ova logika se pokazuje u Zakonu Južne Afrike o promoviranju pristupa informacijama (South Africa's Promotion of Access to Information Act) iz 2002, koji želi „aktivno promovirati društvo u kojemu narodi Južne Afrike imaju učinkovit pristup informacijama koje će im omogućiti potpunije korištenje i zaštitu svih svojih prava."

Pošto je otvorenost neophodni uslov demokratskog upravljanja i zaštite ljudskih prava, izazov u svijetu obavještajnog rada se ne treba definirati kao „iznalaženje prave ravnoteže između tajnosti i transparentnosti". Umjesto toga, tajnost se treba smatrati *izuzetkom koji u svakom pojedinom slučaju iziskuje uvjerljivo opravdanje*. Dok je naglasak obavještajnih zajednica u svijetu na tajnosti sa određenim izuzecima, u demokratskim društvima naglasak bi trebalo staviti na otvorenost, sa određenim izuzecima. Ovo je istovremeno i pitanje principa i pragmatični imperativ. Postoji puno dokaza da su veći izgledi da će se ovlaštenja zloupotrijebiti i ljudska prava kršiti u uslovima tajnosti nego u otvorenom političkom okruženju. Otvorenost omogućuje učinkovit nadzor od strane parlamenta i pažljivo praćenje od strane medija i budnih skupina civilnog društva, dajući osnova za otkrivanje nezakonitosti i zloupotreba, a čime se sprječava razvoj kulture nekažnjivosti.

2.3 RIZIK OD KONKRETNE ŠTETE

Što onda predstavlja adekvatnu osnovu za tajnost obavještajnih službi kao izuzetak od otvorenosti? Uobičajeni odgovor i u demokratskim i u autoritarnim državama je „državna/nacionalna sigurnost". Ovo je neutemeljen i opasan pristup zbog elastičnosti i nejasnosti koncepta „državne/nacionalne sigurnosti."[2] Ako se državna sigurnost tumači tako široko da obuhvati sve aspekte ljudske sigurnosti, onda tajnost koja se zasniva na ovako širokim osnovama može dovesti do pretjeranog i neopravdanog proglašavanja informacija povjerljivima. Čak i kada se „državna sigurnost" definira nešto uže, često se na nju država poziva kada želi opravdati uvođenje novih posebnih mjera koje značajno narušavaju ljudska prava. Na primjer, visoki dužnosnici u Administraciji SAD-a pod predsjednikom Georgeom W. Bushom odobrili su korištenje mučenja u cilju zaštite nacionalne sigurnosti.[3]

Vrhovni sud Sjedinjenih Država je u svojoj presudi iz 1971. godine istakao zabrinutost slične prirode vezano za nejasnoću izraza „državna sigurnost" u odnosu na ograničenje slobode govora:

> *Riječ „sigurnost" je širok, nejasan, opći pojam na čije se konture ne treba pozivati da bi se ukinulo temeljno pravo utjelovljeno u Prvom amandmanu [koji se odnosi na slobodu govora]. Čuvanje vojnih ili diplomatskih tajni na štetu informiranja demokratski izabrane vlade ne doprinosi istinskoj sigurnosti naše Republike.*[4]

U jednoj demokratskoj zemlji, izraz „državna sigurnost" treba obuhvatiti sigurnost zemlje,

njenog sistema vlasti, njenih vrijednosti i svih osoba pod jurisdikcijom te države. Stoga on podrazumijeva obavezu otvorenosti, a ne tajnosti. To nije nešto u odnosu na što treba balansirati ljudska prava i slobode. Demokratski pristup nacionalnoj sigurnosti *obuhvaća i usvaja* ljudska prava i slobode.

Umjesto da se zasniva na nedovoljno jasnom i određenom pojmu „državne sigurnosti", tajnost koja se odnosi na obavještajnu zajednicu se treba zasnivati na to *koja konkretno i koliko značajna šteta* može nastati kad bi došlo do razotkrivanja neke informacije. Treba se ograničiti na ona područja informacija gdje bi razotkrivanje informacije moglo prouzročiti ozbiljnu štetu po živote pojedinaca, obavještajne službe, države, ili zemlje u cjelini. Takve informacije su one koje se odnose na:

- identitet zaposlenih u obavještajnim službama (osim šefova obavještajne službe);
- identitet doušnika obavještajne službe;
- tehničke detalje operativnih metoda;
- detalje zaštite važnih osoba (VIP);
- tekuće operacije i istrage;
- identitet i lične podatke o pojedincima koji su pod prismotrom.

U ovisnosti o okolnostima, šteta koja proistekne iz razotkrivanja informacija koje su vezane za gore navedena područja mora se odvagati u odnosu na snažan javni interes da se informacije objavljuju. Objavljivanje u javnom interesu može biti odgovarajuća mjera ukoliko su, na primjer, obavještajne operacije nezakonito usmjerene na političare, zaštita koja se dodjeljuje VIP osobama je izuzetno slaba, ili su se visoki obavještajni dužnosnici osobno ponašali na vrlo kompromitirajući način. Generalno govoreći, vlade ne mogu nastojati izbjeći svaku moguću štetu koja će nastati od objavljivanja osjetljivih informacija. Određeni nivo štete se mora tolerirati jer bi tajnovitost mogla dovesti u opasnost sam demokratski poredak.

Javnost i parlament kao cjelina treba da imaju ograničeniji pristup informacijama o obavještajnoj zajednici nego pristup koji uživaju specijalizirana nadzorna tijela nad obavještajnim službama, kao što je parlamentarni odbor za nadzor ili neovisni generalni inspektor za obavještajne službe. Da bi ispunili svoj mandat, ova tijela trebaju više informacija nego što se pušta u domenu javnost. U nastavku poglavlja razmatraju se potrebe ovih tijela za informacijama.

2.4 PRAKTIČNE KORISTI OD OTVORENOSTI OBAVJEŠTAJNIH SLUŽBI

Prethodna diskusija se fokusirala na potrebu za otvorenošću obavještajnih službi u smislu demokratskog upravljanja, poštivanja ljudskih prava i sprječavanja zloupotrebe ovlaštenja. Ali osim toga, manje tajnovitosti i pružanje više informacija o obavještajnim službama bilo bi od koristi i samim službama. Sistem koji previše informacija klasificira kao povjerljive nema dovoljan kredibilitet, težak je za održavanje i provođenje, a usto je skup i neučinkovit. Previše vremena i napora odlazi na klasificiranje i zaštitu bezazlenih informacija, što potencijalno može ići na štetu zaštite istinski osjetljivih informacija.

U poznatoj presudi Vrhovnog suda Sjedinjenih Država iz 1971. godine u predmetu Dokumenti iz Pentagona (The Pentagon Papers), sudac Potter Stewart je u vezi s ovim rekao slijedeće:

> *Kada je sve proglašeno povjerljivim, onda ništa nije povjerljivo, i sistem postaje nešto što cinici i oni koje nije briga ne poštuju, a oni koji nastoje ostvariti samozaštitu ili samopromociju njime manipuliraju.*[5]

Štoviše, kako je već spomenuto u uvodu, veća transparentnost u pogledu obavještajnih službi bi pomogla smanjenju sumnjičavosti koje javnost gaji prema ovim organizacijama i osnažilo povjerenje javnosti prema njima. To je od vitalnog značaja u demokratiji s obzirom da obavještajne agencije moraju dobivati informacije od pojedinaca i zajednica kroz odnose suradnje, a ne zastrašivanjem i prinudom.

3. ZAKONI O ZAŠTITI I PRISTUPU INFORMACIJAMA

U demokratskim zemljama, debata o tajnosti i transparentnosti obavještajnih službi koja je razmatrana u gornjem tekstu nikada nije konačno i trajno riješena. Ona može biti mjesto borbe, posebno u vrijeme krize obavještajnih službi i obavještajnih skandala, a klatno se može njihati ka većoj otvorenosti ili većoj tajnosti, u zavisnosti od političkih i sigurnosnih uslova u zemlji, ponašanju obavještajnih službi, i perspektiva izvršne vlasti, parlamenta i javnosti.

Ipak, u formalnom smislu, ova se debata rješava zakonima koji se bave pristupom i zaštitom informacija u posjedu države. Ovi zakoni obično obuhvaćaju slijedeće teme:

- načela i kriterije za klasificiranje i objavljivanje informacija;
- nadležnost organa i procedure za klasifikaciju i skidanje de-klasifikaciju;
- revizija klasifikacije od strane suda ili nekog drugog organa;
- pravo pojedinaca i grupa koje rade u javnom interesu da ostvare pristup informacijama u posjedu države;
- procedure za podnošenje zahtjeva za ostvarivanje takvog prava i pravo žalbe ukoliko se pravo pristupa uskrati;
- uloga sudova u presuđivanju sporova vezanih za klasifikaciju informacija i pristup istim;
- kazne za nezakonito razotkrivanje informacija.

Obavještajne službe su obično odgovorne za klasifikaciju informacija u posjedu države i za uspostavu i održavanje sistema zaštite klasificiranih informacija. Također, one mogu biti uključene i u izradu zakona. Time se stvara opasnost da će zakon naginjati pretjeranoj tajnovitosti. Pošto su obavještajne službe funkcionalno sklone tajnovitosti i protivne otvorenosti, odgovornost za izradu zakona bi trebala biti na ministarstvu pravde ili ustavnih poslova.

Parlament i njegovi odbori za nadzor, kao što su oni koji se bave ustavnim pitanjima i obavještajnim službama, imaju odlučujuću ulogu u tome da se pobrinu da zakon bude u skladu sa demokratskim normama. Oni mogu unaprijediti kvalitet i demokratski karakter zakona tako što će pozivati izvršnu vlast da predstavi javnosti motive na kojima se zakon zasniva, kao i sve kontroverzne odredbe; omogućavanjem zdrave debate između političkih stranaka; održavanjem javnih rasprava koje će omogućiti pojedincima, medijima i drugim interesnim grupama da komentiraju nacrt zakona; i unošenjem odgovarajućih izmjena u zakon. Na kraju krajeva, parlament je nadležan za usvajanje zakona.

U mladim demokratskim državama parlamentarni zastupnici bi mogli imati koristi od komparativnog međunarodnog pregleda čiji bi cilj bio utvrđivanje najboljih praksi.[6] Za slijedeće se može reći da predstavljaju dobre prakse kad se radi o zakonima koji reguliraju pristup i zaštitu informacija:

- Zakon treba izričito istaći značaj transparentnosti i pristupa informacijama kao temeljno načelo demokratije koje promovira ljudska prava i slobode, dobro upravljanje, odgovornost prema javnosti i raspravu na osnovu dovoljno informacija. Zakon treba navesti da klasifikacija informacije kao povjerljive stoga predstavlja izuzetnu mjeru koja se mora oprezno koristiti.
- Zakon treba izrijekom nastojati spriječiti neopravdana ograničenja pristupa informacijama (Okvir 1).
- Kriteriji za klasificiranje informacija povjerljivima trebaju navesti da bi moglo doći do nastanka značajne štete, uz razuman nivo pouzdanosti, ako bi došlo do razotkrivanja informacije. Zakon ne bi smio dopustiti pribjegavanje tajnovitosti na maglovitim osnovama „državne sigurnosti“ ili „nacionalnog interesa“.
- Kriteriji koji se odnose na objavljivanje, odnosno neobjavljivanje informacija treba da budu precizni i jednostavni da bi vladinim dužnosnicima bilo moguće da pravilno i dosljedno donose odluke i osiguraju da su pojedinci svjesni da mogu iskoristiti svoje pravo na informacije u posjedu države.
- Zakon treba predvidjeti ocjenu statusa klasificiranih informacija u određenim intervalima (npr. svakih pet godina) i nadležni dužnosnici trebaju informirati javnost o rezultatima tih ocjena.
- Kada se odbije nečiji zahtjev za informacijom u posjedu države, nadležni dužnosnik mora informirati podnositelja o razlozima za nedavanje informacije i koliko dugo će se informacija smatrati klasificiranom odnosno povjerljivom. Zakon treba predvidjeti da podnosilac, ako ima legitiman lični ili javni interes, može tražiti od nadležnog dužnosnika da informaciju proglasi deklasificiranom. Kada neki dužnosnik odbije takav zahtjev, podnosilac treba imati pravo žalbe na takvu odluku. Žalbu treba razmotriti sudija.
- Zakon treba predvidjeti da se klasificiraju i smatraju povjerljivom *informacije*, a ne *dokumenti*. Na ovaj način se vladinim dužnosnicima omogućava da klasificiraju osjetljive informacije u dokumentu, a da pri tom ne moraju klasificirati cijeli dokument kao povjerljiv. Takvi se dokumenti onda mogu objaviti u prečišćenoj formi.
- Kada su klasificirane informacije relevantne za neki sudski postupak, odluku o tome da li će se te informacije razmatrati iza zatvorenih vrata (*in camera*) ili javno treba donijeti sudija, a ne predstavnik izvršne vlasti.
- Zakon treba omogućavati osobama optuženim za nezakonito razotkrivanje klasificiranih informacija da se u svoju odbranu pozovu na otkrivanje „u javnom interesu“. Ovo se može desiti kada, na primjer, novine otkriju detalje nezakonitog prisluškivanja od strane obavještajne agencije. Validnost odbrane pozivanjem na javni interes će utvrditi sudija koji razmatra predmet.
- Zakon treba propisati obavezu izvršne vlasti da poduzme korake za promoviranje i olakšavanje pristupa javnosti informacijama u posjedu države, uključujući, što se razmatra u nastavku, informacije o obavještajnim službama.

Navedeni elementi zakona koji odražavaju dobre prakse jednako se odnose na proceduralna kao i na sadržinska pitanja i odnosi se na informacije u posjedu države koje uključuju, ali se

ne ograničavaju, na obavještajnu zajednicu. Naredni odjeljci se bave sadržinskim aspektima obavještajnih podataka koji se trebaju staviti na uvid različitim tijelima za nadzor.

Okvir 1: Zabrana neopravdane klasifikacije informacija kao tajnih

Izvršna uredba Sjedinjenih Država o klasifikaciji navodi da se neka informacija ne može klasificirati kao povjerljiva da bi se prikrila povreda zakona, neefikasnost ili administrativna greška, spriječilo sramoćenje neke osobe, organizacije ili agencije; i ne smije se sprječavati ili odlagati objavljivanje informacije koja ne iziskuje zaštitu u cilju interesa državne sigurnosti. Isto tako, Slovenački zakon o zaštiti klasificiranih informacija zabranjuje klasificiranje neke informacije kao povjerljive ukoliko se ona odnosi na kršenje ljudskih prava i međunarodnih zakona.[7]

4. POTREBE PARLAMENTA ZA INFORMACIJAMA

U demokratskoj državi, institucija na kojoj leži primarna odgovornost za nadzor djelovanja izvršne vlasti i državnih odjela je parlament. Da bi parlament mogao obavljati ovu svoju funkciju u odnosu na obavještajne službe, mora raspolagati sljedećim informacijama: prioritetima obavještajnih službi; politikama, propisima i radnjama izvršne vlasti koje se odnose na obavještajne službe; obavještajnim procjenama, budžetima i finansijskim izvještajima; izvještajima institucije vrhovne revizije u zemlji o obavještajnim službama; aktivnostima i nalazima stručnih nadzornih tijela nad obavještajnim službama; kao i svim istragama koje se odnose na vršenje obavještajne službe. Ovaj odjeljak se bavi informacijama koje parlament treba kada zasjeda na otvorenoj sjednici, za razliku od parlamentarnih odbora za nadzor obavještajnih službi, koji su razmatrani ranije.

4.1 DRŽAVNI OBAVJEŠTAJNI PRIORITETI

Povremeno, obično na godišnjoj osnovi, izvršna vlast mora donijeti odluku o tome koji će biti obavještajni prioriteti u narednom razdoblju. Razlog za ovo je taj što obavještajne službe ne treba same sebi određivati zadaću, jer je određivanje prioritetnih prijetnji i područja na koja će se fokusirati obavještajni rad pitanja za visoki politički nivo. Utvrđivanje obavještajnih prioriteta od strane izvršne vlasti daje politički pravac službi i služi kao osnova za planiranje, izradu budžeta, raspodjelu resursa, operacije i odgovornost.

Nacionalni prioriteti izvršne vlasti (NPI) ne trebaju biti klasificirani kao tajni. Rasprave u parlamentu o NPI produbljuju odgovornost i demokratsko odlučivanje o tom aspektu državne politike koji tako duboko utječe na sigurnost i dobrobit osoba pod jurisdikcijom države. Njihovo otkrivanje neće ugroziti državnu sigurnost pošto se NPI mogu dostaviti parlamentu bez navođenja imena konkretnih osoba i organizacija, gdje se umjesto imena i naziva koriste opće kategorije kao što je „organizirani kriminal“, „terorizam“ i „širenje posjedovanja nuklearnog naoružanja.“

Osjetljive informacije se mogu izostaviti iz verzije NPI koja se predstavlja parlamentu, i mogu se dostaviti na povjerljivoj osnovi parlamentarnom odboru za nadzor nad obavještajnim službama.

4.2 POLITIKE, PROPISI I AKCIJE IZVRŠNE VLASTI

Izvršne politike i propisi koji se odnose na obavještajne službe su često tajne, čak i u dobro uspostavljenim demokratijama. To predstavlja anomaliju i nije poželjno zato što narušava suštinski princip odgovornosti. Primarna pravila koja reguliraju rad obavještajnih službi, posebno kad se radi o istražnim postupcima koji ograničavaju ustavna prava, moraju biti predmet parlamentarne rasprave i razmatranja. Potrebno je napraviti razliku između unutarnjih pravila odjela i procedura koji se moraju smatrati tajnima jer otkrivaju osjetljive tehničke detalje operativnih metoda, i propisa i politika izvršne vlasti koji bi trebalo da budu u domenu javnosti s obzirom da su integralni dio demokratskog upravljanja.

Na osnovu zakona o obavještajnim službama, izvršna vlast treba predstaviti parlamentu na razmatranje i kritiku svoje politike i propise o sljedećim pitanjima:

- vršenju funkcije i ovlaštenja obavještajnih organizacija, uključujući ovlaštenje da ograničava ustavna prava;
- operativnim politikama, izuzev osjetljivih tehničkih podataka;
- ministarskoj kontroli i odnosu između obavještajnih službi i šefa države, kabineta i ministra nadležnog za obavještajne službe;
- odnosu i podjeli nadležnosti između različitih obavještajnih tijela, koordinaciji obavještajnog rada i funkcijama svih obavještajnih koordinacijskih mehanizama u državi;
- odnosima sa stranim obavještajnim službama i kriterijima i pravilima za razmjenu obavještajnih informacija o pojedincima sa stranim vladama;
- disciplinskom sistemu obavještajnih službi i unutarnjim mehanizmima za osiguranje poštivanja ustavnosti i zakonitosti

Parlament je odgovoran za nadziranje izvršnih, kao i državnih institucija. Iz tog razloga mu trebaju informacije o značajnim radnjama izvršne vlasti koje se odnose na obavještajne službe. Relevantne radnje obuhvaćaju imenovanje i smjenu visoko pozicioniranih osoba; disciplinske radnje protiv visoko pozicioniranih osoba; ministarska odobrenja posebnih operacija gdje je to propisano zakonom (vidjeti Poglavlje 5 – Hutton); i značajne reforme i inovacije koje se odnose na sisteme i operacije obavještajnih službi. Informacije koje su previše osjetljive da bi bile puštene u domenu javnosti trebaju se dostavljati parlamentarnom odboru za nadzor nad obavještajnim službama.

4.3 GODIŠNJI IZVJEŠTAJI OBAVJEŠTAJNIH SLUŽBI

U demokratiji je objavljivanje godišnjih izvještaja od strane vladinih odjela i drugih državnih organa neophodno sredstvo osiguranja odgovornosti prema parlamentu i općenito javnosti. Na taj način parlament stječe osnovu za utvrđivanje da li se poštuju vladini prioriteti i da li porezni obveznici dobivaju adekvatnu uslugu za svoj novac. Ne postoji opravdan razlog da se iz ove prakse izuzmu obavještajne službe. Godišnji izvještaj Holandske opće obavještajne i sigurnosne službe (AIVD) predstavlja izvrstan primjer davanja sveobuhvatnih i korisnih informacija pri čemu se ne ugrožava državna sigurnost.[8]

Godišnji izvještaji obavještajnih službi treba da obuhvate sljedeća pitanja (bez otkrivanja osjetljivih detalja): godišnji zadaci i prioriteti službe; njena procjena najvažnijih prijetnji po sigurnost; sve značajne reforme obavještajnih politika, sistema i operacija; ispunjavanje

funkcije izvještavanja i odgovornosti službe; i odgovore službe na zahtjeve za informacije prema zakonu o slobodi informiranja.

4.4 OBAVJEŠTAJNE PROCJENE

U velikom broju slučajeva procjene obavještajnih službi koje se odnose na pojedince i organizacije nisu podesne za podnošenje parlamentu zbog rizika da će se ugroziti obavještajne operacije i krivične istrage. Ipak, obavještajne procjene koje se bave kategorijama sigurnosti i prijetnji sigurnosti se mogu objavljivati često bez izlaganja riziku štete.

Na primjer, Kanadska sigurnosno-obavještajna služba (Canadian Security Intelligence Service - CSIS) objavljuje niz materijala među kojima su: razmatranja na teme poput ekonomske sigurnosti, rastućeg posjedovanja naoružanja, i anti-terorističke aktivnosti; publikacija koja se naziva *Komentar* (*Commentary*) i koja se fokusira na pitanja koja se odnose na sigurnost Kanade; i seriju studija zasnovanih na procjeni informacija iz otvorenih izvora koje vrši CSIS.[9] Godišnji izvještaj Holandske opće obavještajne i sigurnosne službe (Dutch General Intelligence and Security Service) ide čak tako daleko da uključuje komentare o radikalnim i terorističkim organizacijama koje se navode imenom.[10]

Predstavljanje ovih procjena parlamentu i njegovom odboru (odborima) za nadzor nad obavještajnim službama predstavlja važan oblik odgovornosti, čime se parlamentarnim zastupnicima, akademskoj javnosti i nevladinim organizacijama omogućuje da raspravljaju o političkim i sigurnosnim perspektivama obavještajnih službi. Vremenom, parlamentarna i javna diskusija zasnovana na pravim informacijama može dovesti do rafiniranja tih perspektiva.

4.5 BUDŽETI, FINANSIJSKI IZVJEŠTAJI I IZVJEŠTAJI INSTITUCIJA VRHOVNE REVIZIJE

U demokratskim zemljama parlament dobiva, razmatra i raspravlja o godišnjim budžetima i finansijskim izvještajima vladinih tijela. Ovo je prijeko potrebni oblik odgovornosti i polaganja računa koji omogućuje izabranim predstavnicima naroda da nadzire i odobrava korištenje javnih sredstava u skladu sa zakonom, vladinim politikama i vlastitim prioritetima i preferencama parlamenta. Međutim, cjelovita verzija finansijskih izvještaja i budžeta obavještajnih službi se obično podnosi na povjerljivoj osnovi samo parlamentarnim odborima za nadzor nad obavještajnim službama i ne stavlja se na dnevni red parlamentu u cjelini (vidjeti Poglavlje 8 – Wills).

Obavještajne organizacije se protive otkrivanju svojih budžeta smatrajući da bi tako strane obavještajne službe stekle određenu prednost u odnosu na njih. Ovaj argument je pretjeran. Strana agencija nema nikakvu korist od informacije o tome koliko neka druga zemlja troši na svoja obavještajna tijela. Niti bi bilo kakva prednost ili lošija pozicija po službu proistekla iz objavljivanja koliko je potrošeno na zaposlene, operativne troškove i kapitalne rashode. Tek na mnogo većem nivou detalja – koji se odnose na ciljeve, metode, izvore i operativne ishode i ograničenja – bi moglo doći do podrivanja sigurnosti zbog razotkrivanja ovih informacija (vidjeti Okvir 2).

Okvir 2: Objavljivanje budžeta i finansijskih izvještaja obavještajnih službi

Ministarska komisija za ocjenu obavještajnih službi u Južnoj Africi je 2006. godine pažljivo razmotrila klasificirane budžete, finansijske izvještaje i strateške planove koje na godišnjoj osnovi podnose obavještajne službe parlamentarnom odboru za nadzor obavještajnih službi. Komisija je zaključila da objavljivanje ovih dokumenata ni na koji način neće ugroziti obavještajne operacije niti sigurnost zemlje. Komisija se složila sa stavom Državnog trezora da budžeti i finansijski izvještaji obavještajnih službi treba da budu otvoreno predstavljeni parlamentu. Osjetljivi detalji se mogu ograničiti na dokumente koji se razmatraju na zatvorenim sjednicama odbora za nadzor.[11]

Isto tako, godišnji izvještaj tijela vrhovne revizije o obavještajnim službama treba biti rađen u dvije verzije: javni izvještaj, koji se dostavlja parlamentu, i klasificirani izvještaj, u kojemu se navodi više detalja i koji se podnosi parlamentarnom odboru za nadzor. Zakon koji regulira izvještaje glavnog revizora treba predvidjeti zaštitu osjetljivih informacija (vidjeti Okvir 3).

Okvir 3: Zaštita osjetljivih informacija u finansijskoj reviziji

Zakon o javnoj reviziji Južne Afrike (South Africa's Public Audit Act) iz 2004. godine sadrži nekoliko odredbi koje se odnose na zaštitu osjetljivih informacija. U njemu se navodi da glavni revizor mora poduzeti mjere opreza da osigura zaštitu od objavljivanja tajnih ili povjerljivih informacija za koje je saznao tokom vršenja revizije. Kod izvještavanja o povjerljivom računu koji se odnosi na sigurnost, glavni revizor „mora uvažiti posebnu prirodu tog računa i, na osnovu pismenog savjeta nadležnog Ministra, a na osnovu nacionalnog interesa, može isključiti povjerljive, tajne ili klasificirane detalje iz zaključaka izvještaja o reviziji, pod uslovom da se u izvještaju navede da su izostavljeni ti detalji."

4.6 POSTUPANJE U SLUČAJEVIMA SKANDALA U KOJE SU UKLJUČENE OBAVJEŠTAJNE SLUŽBE

Prethodna diskusija se fokusirala na obavještajne informacije koje parlament treba kako bi mogao ispuniti svoju obavezu nadzora. Ukoliko nastupi neka kriza koja uključuje obavještajne službe (npr. otkrivanje špijuniranja političara), parlament može uspostaviti istražnu komisiju ili zatražiti od nekog od specijaliziranih nadzornih tijela rada obavještajnih službi da provede istragu. Zaključke istrage treba prezentirati i o njima parlament treba otvoreno raspravljati. Ukoliko se ovo ne radi otvoreno, javnost neće imati povjerenja u istrage i neće postojati uvjerenje javnosti da su poduzete adekvatne mjere u svim slučajevima utvrđenih nepravilnosti.

5. POTREBE SPECIJALIZIRANIH NADZORNIH TIJELA OBAVJEŠTAJNIH SLUŽBI ZA INFORMACIJAMA

Potrebe za informacijama specijaliziranih nadzornih tijela nad obavještajnim službama – među kojima primarno mjesto ima parlamentarni odbor za nadzor nad obavještajnim službama, neovisni generalni inspektor za obavještajne službe i stručno nadzorno tijelo nad obavještajnim službama (kao što je Odbor za ocjenu rada obavještajnih i sigurnosnih službi u Holandiji) – proistječu iz mandata i funkcija tih tijela. Taj mandat i funkcije su

različite u svakoj zemlji, ali se može odnositi na sljedeće:

- da li obavještajne službe poštuju ustav, zakone, propise i vladine politike;
- rezultate i uspjehe obavještajnih službi u smislu njihovog zakonskog mandata i funkcija, kao i prioriteta koje utvrđuje vlada;
- interne sisteme i metode sprječavanja, otkrivanja i postupanja u slučaju zloupotrebe;
- interni finansijski sistemi i trošenje.

U svjetlu ovih funkcija nadzora, ovaj odjeljak se bavi time koje su informacije potrebne parlamentarnom odboru za nadzor nad obavještajnim službama, neovisnom generalnom inspektoru za obavještajne službe i drugim institucijama ombudsmena, te sudstvom. U odjeljku se potom prolazi kroz načine smanjenja rizika od nenamjernog ili namjernog otkrivanja povjerljivih informacija.

5.1 PARLAMENTARNI ODBORI ZA NADZOR NAD OBAVJEŠTAJNIM SLUŽBAMA

Parlamentarni odbor za nadzor nad obavještajnim službama bi po prirodi stvari bi trebalo da dobije sve informacije o obavještajnom radu koje se dostavljaju parlamentu u cjelini. On bi trebalo obično prvi da dobije te informacije kako bi imao priliku, prije rasprave u parlamentu, da ostvari detaljan uvid, razmatanje i interakciju sa visokim obavještajnim dužnosnicima i članom (članovima) izvršne vlasti koja je nadležna za obavještajne službe. Odbor, kao kolektiv, a isto tako i njegovi članovi koji predstavljaju različite političke stranke, tako dolaze u priliku da mogu dati dobro informiran doprinos široj raspravi u parlamentu.

Osim toga, odbor za nadzor treba da dobije, na povjerljivoj osnovi, detaljnije i osjetljivije informacije od onih koje se dostavljaju parlamentu kao cjelini. Teme o kojima treba da dobije detaljne informacije uključuju sljedeće:

- državne obavještajne prioritete izvršne vlasti;
- politike, propise i radnje izvršne vlasti koje se odnose na obavještajne službe;
- godišnje izvještaje obavještajnih službi;
- sigurnosne procjene i prijetnje koje su sačinile službe;
- godišnje budžete i finansijske izvještaje službi;
- izvještaje vrhovnih institucija za reviziju koje se odnose na obavještajne službe;
- aktivnosti i zaključke stručnih nadzornih tijela obavještajnih službi (ukoliko isti postoje).

Ovdje je najvažnije i najteže pitanje koliko detalja i koji nivo osjetljivosti se treba dostavljati nadzornom odboru. S jedne strane, članovi ovog odbora nisu obučeni da čuvaju tajnost i zasigurno imaju pomiješan osjećaj lojalnosti prema svojoj zemlji i prema svojoj političkoj stranci. Dalje, važi aksiom da što je veći broj ljudi koji su upoznati sa nekom tajnom informacijom, to je manje vjerovatno da će ta informacija ostati tajnom. Obavještajne službe stoga nevoljko otkrivaju osjetljive podatke o svojim operacijama, metodama i ljudima. S druge strane, parlamentarni odbor mora dobiti dovoljno detaljne informacije da može adekvatno vršiti svoje funkcije nadzora. Ukoliko se uskrati previše informacija, nadzor će biti površan i neće otkriti niti pravilno ispitati nezakonite radnje, loše rezultate ili nenamjensko korištenje sredstava.

Na pitanje koliko detalja i koji nivo osjetljivosti se treba predstaviti odborima za parlamentarni nadzor, odgovor treba dati u zakonu, i to što preciznije, kako bi se na minimum svela mogućnost nastanka nesporazuma i sporova između parlamenta i obavještajnih službi i/ili izvršne vlasti. Način na koji se ova pravila i smjernice formuliraju u zakonu razlikuje se od zemlje do zemlje (vidjeti Okvir 4, gdje se navodi nekoliko primjera).

Osim toga, zakon treba detaljno precizirati načine rješavanja sporova vezanih za dostavljanje informacija parlamentarnom odboru. U Južnoj Africi, na primjer, relevantni zakon predviđa da će sporove rješavati ad hoc odbor kojeg će činiti ministar za obavještajne službe, šef obavještajne službe, predsjedavajući parlamentarnog odbora za nadzor i generalni inspektor za obavještajne službe.[12]

Prava parlamentarnog odbora za nadzor da dobije informacije koje se odnose na obavještajni rad razlikuju se od zemlje do zemlje. U svakom slučaju, odbor bi trebalo da dobija redovne izvještaje od: članova izvršne vlasti koji su nadležni za obavještajne službe; obavještajnih službi; institucija vrhovne revizije; sudije ili člana izvršne vlasti koji je odgovoran za odobravanje posebnih mjera; i izvještaje svih tih tijela. Osim toga, može raspolagati ovlaštenjima da vodi istrage, da poziva svjedoke i da vrši inspekciju prostorija obavještajnih službi.

Okvir 4: Zakonske odredbe o pristupu informacijama koje se odnose na parlamentarne odbore za nadzor

U Rumuniji, obavještajne službe imaju obavezu da ispune zahtjeve za informacijama koje im uputi odbor za nadzor obavještajnih službi u razumnom roku, osim u slučaju kada bi to ugrozilo tekuće operacije, identitet agenata, metode ili izvore. Parlamentarni odbori mogu dolaziti u nenajavljene posjete službi i mora im se omogućiti neograničeni pristup osoblju, podacima i prostorijama.[13] U Ujedinjenom Kraljevstvu, za razliku od toga, trenutni mandat parlamentarnog odbora za nadzor je ograničen na „troškove, administraciju i politiku“ obavještajnih i sigurnosnih službi, čime se implicitno iz područja nadležnosti odbora izuzimaju operacije, čime se ograničava pristup odbora informacijama.[14]

5.2 GENERALNI INSPEKTOR ZA OBAVJEŠTAJNE SLUŽBE I DRUGE INSTITUCIJE OMBUDSMENA

Tajnovitost koja okružuje obavještajne službe postavlja značajne teškoće u vršenju učinkovitog nadzora. Zbog toga, postoji potreba za nadzornim tijelima nad obavještajnim službama koja imaju posebna ovlaštenja i stručna znanja. Jedno takvo tijelo je generalni inspektor za obavještajne službe (GI).[15] Da bi obavljao učinkovit nadzor u okruženju tajnosti, GI mora imati sljedeće karakteristike:

- GI mora biti neovisni dužnosnik sa sigurnim mandatom;
- On/ona mora imati zakonom utvrđen mandat da prati da li službe poštuju ustav, zakone i vladine politike, kao i da istražuje žalbe na loše ponašanje, nezakonite radnje i zloupotrebu ovlaštenja;
- GI mora podnositi izvještaje ne samo ministru nadležnom za obavještajne službe, nego i parlamentarnom odboru za nadzor nad obavještajnim službama i, kada se radi o važnim istragama, parlamentu u cjelini;
- GI i njegovo/njeno osoblje mora posjedovati visoki nivo stručnosti i iskustva u obavještajnom radu.

Osim navedenog, zakon koji regulira GI mora predvidjeti da se generalnom inspektoru i njegovom osoblju ne može uskratiti pristup bilo kojem obavještajnom podatku, informaciji ili prostorijama koje su pod kontrolom obavještajnih službi, te da svako takvo uskraćivanje pristupa predstavlja krivično djelo. To su najvažniji zahtjevi koji se moraju ispuniti kada neovisno nadzorno tijelo istražuje tajne operacije i obavještajne sisteme.

Gornji komentari o GI jednako se tako odnose na druge institucije ombudsmena, kao što su povjerenici za ljudska prava, u zemljama gdje ne postoji generalni inspektor za obavještajne službe. Velika prednost ovakvog specijalističkog pristupa GI je u tome što generalni inspektor i njegovo osoblje posjeduju stručnost za obavještajni rad, što ih čini sposobnima da uoče nepravilnosti u tajnom okruženju i da pravilno zaštite povjerljive informacije kojima imaju pristup.

Kad vrše reviziju potrošnje, raspodjele budžeta, prihoda (ako postoji) i finansijskih sistema obavještajnih službi, institucije vrhovne revizije treba da imaju pristup svim informacijama koje se odnose na tajne operacije službi (više informacija potražiti u Poglavlje 8 – Wills). Prema tome, institucije vrhovne revizije trebaju imati specijalni tim koji je obučen za rad sa povjerljivim dokumentima, te je prošao i sigurnosne provjere. Kao alternativa, može se smatrati podesnim da ured neovisnog generalnog inspektora za obavještajne službe vrši finansijsku reviziju u saradnji sa institucijom vrhovne revizije.

5.3 SUDSTVO

Obavještajne službe i agencije za provođenje zakona krše pravo na privatnost kada obavljaju posebne radnje kao što je presretanje komunikacije, pretresanje i konfiskacija. Kao posljedica toga, u većini demokratskih zemalja vladini organi moraju dobiti odobrenje suda da bi mogli pristupiti vršenju tih operacija (vidjeti Poglavlje 5 – Hutton, u kojoj se ovo pitanje dalje razmatra). U ovisnosti o zemlji, agencije mogu imati pravo pristupiti bilo kojem sudiji u ove svrhe, ili može postojati određeni sudija koji razmatra sve zahtjeve za presretanje informacija.

Informacije koje će sudiji u tu svrhu trebati su obično predviđene zakonom o presretanju komunikacija. Podnositelj zahtjeva mora predočiti dovoljno činjenica koje će uvjeriti sudiju da je presretanje neophodno i opravdano sredstvo skupljanja informacija o kriminalnoj aktivnosti ili prijetnji po državnu ili javnu sigurnost. Zakon može predvidjeti da je presretanje komunikacija metoda kojoj se pribjegava kao posljednjem sredstvu, i u tom slučaju podnositelj zahtjeva mora također uvjeriti sudiju da uobičajene metode nisu dovoljne ili nisu podesne.

Osim podnošenja zahtjeva za presretanje, obavještajne službe se mogu naći pred sudovima u krivičnim i građanskim predmetima ukoliko, na primjer, neka osoba koja radi u obavještajnoj službi bude optužena za neko djelo, ili neki političar ustvrdi da mu/joj je ured bio nezakonito prisluškivan. Izvršna vlast može željeti da neki ili svi takvi predmeti budu razmatrani iza zatvorenih vrata (*in camera*). Demokratije se između sebe razlikuju po tome kako pristupaju ovom problemu. Pitanje može biti propisano zakonom, ili se može prepustiti nahođenju predsjedavajućeg sudije (Okvir 5).

Okvir 5: Postupanje sa osjetljivim informacijama u sudskom postupku

U predmetu kojeg je razmatrao Ustavni sud Južne Afrike 2008. godine, jedna novinska grupa je tražila da sud naloži objavljivanje povjerljivih dijelova zapisnika sa sudskih postupaka koji su se odnosili na Državnu obavještajnu agenciju (National Intelligence Agency ili NIA). Svoj je zahtjev zasnivala na pravu na otvorenost suđenja. Ministar obavještajnih službi se usprotivio objavljivanju, pozivajući se pri tom na državnu sigurnost. Sud je naložio da se dio materijala objavi, navodeći da razlozi državne sigurnosti ne daju valjanu osnovu da se to ne učini, ali je također zauzeo stav da neke druge informacije – one koje se odnose na odnose sa obavještajnim službama drugih država, komandni lanac unutar NIA i identitet NIA operativaca – ostanu povjerljive. Mišljenje da je u javnom interesu da se objavi cjelokupni materijal osim imena određenih operativaca ostalo je u manjini.[16]

5.4 UNAPRJEĐENJE ODGOVORNOSTI NADZORNIH TIJELA

Demokratske zemlje mogu imati relativno snažan parlamentarni i neovisni nadzor nad obavještajnim službama, a da ipak nadzorna tijela možda nisu adekvatno odgovorna prema javnosti. I sama nadzorna tijela mogu biti previše tajnovita. Time se podriva povjerenje javnosti kako u nadzorna tijela tako i u obavještajne službe. Stoga je na nadzornim tijelima da predoče suvisle izvještaje parlamentu i da objave svoje izvještaje kao i izvještaje obavještajnih službi na svojoj internet stranici. Dobar primjer ovoga je Odbor za ocjenu rada obavještajnih i sigurnosnih službi Holandije koji svake godine objavljuje sveobuhvatan izvještaj o monitoringu i istragama koje vrši.[17]

5.5 SMANJENJE RIZIKA OD OBJAVLJIVANJA KLASIFICIRANIH INFORMACIJA

Kako je ranije već spomenuto, obavještajne službe se katkad protive objavljivanju osjetljivih informacija parlamentarnim tijelima za nadzor jer su članovi tih odbora političari i obično ne posjeduju disciplinu i nemaju iskustvo potrebno za čuvanje povjerljivih informacija. Stoga se pojavljuje rizik od namjernog ili nenamjernog razotkrivanja osjetljivih informacija. U cilju svođenja tog rizika na minimum mogu se poduzeti sljedeći koraci:

- zakon o zaštiti informacija propisuje da je neovlašteno otkrivanje informacija koje su klasificirane kao povjerljive krivično djelo;
- članovi parlamentarnih odbora za nadzor prolaze sigurnosne provjere (eng. vetting) od strane obavještajne službe prije nego što budu imenovani u odbor;[18]
- odbori su zakonom ovlašteni da se sastaju iza zatvorenih vrata;
- obavještajni stručnjaci se brinu da uredi, računari, telefoni i sistemi čuvanja dokumentacije budu zaštićeni od prisluškivanja/neovlaštenog uvida;
- obavještajni stručnjaci obučavaju članove i zaposlenike u tim odborima;
- odbori i obavještajne službe zajednički usvajaju pravila i procedure koji se odnose na primanje, posjedovanje, korištenje i uništavanje klasificiranih informacija.

Gore navedene mjere su u cijelosti ili u nekom dijelu također relevantne i za druga specijalizirana nadzorna tijela. Međutim, kada ova tijela u svom sastavu imaju profesionalce, a ne političare, rizik objavljivanja klasificiranih informacija je možda manji.

6. PREPORUKE

- Transparentnost i slobodan pristup informacijama u posjedu države predstavljaju neophodni uslov za demokratsko upravljanje, zaštitu ljudskih prava i prevenciju zloupotrebe ovlaštenja. Tajnost se stoga treba smatrati izuzetkom. Što se tiče obavještajnih službi, tajnost se treba zasnivati na konkretnoj i značajnoj šteti koja bi mogla nastati kao posljedica objavljivanja informacija. Stoga se treba ograničiti samo na ona područja gdje bi otkrivanje informacija prouzročilo ozbiljnu štetu po živote osoba, obavještajne službe, državu ili zemlju u cjelini. Šteta koja bi nastala otkrivanjem informacija se mora izbalansirati u odnosu na prevlađujuće pravo javnosti za pristup informacijama u posjedu državnih organa.

- Odgovornost za izradu zakona o zaštiti i pristupu informacijama treba biti na ministarstvu pravde ili tijela nadležnih za pravna pitanja, a ne na obavještajnim službama. Parlament treba nastojati osigurati da zakoni budu u skladu sa demokratskim normama.

- Zakon treba naglašavati da su transparentnost i pristup informacijama temeljna načela i da je klasifikacija informacija nešto što se mora koristiti s oprezom. Kriteriji za klasifikaciju treba jasno da ukazuju na to koja mjera štete je dovoljna da se opravda uskraćivanje objavljivanja informacija Zakon treba omogućiti osobi koja je optužena za nezakonito razotkrivanje klasificiranih informacija da se u svoju odbranu poziva na javni interes. Izvršna vlast se treba obavezati da promovira i olakša pristup javnosti informacijama u posjedu države, uključujući tu informacije o obavještajnim službama.

- Parlament treba informacije o sljedećem: obavještajnim prioritetima; izvršnim politikama, propisima i aktivnostima obavještajnih službi; obavještajnim procjenama, budžetima i finansijskim izvještajima; izvještajima institucija vrhovne revizije o obavještajnim službama; aktivnostima i zaključcima stručnih nadzornih tijela; i svim istragama ponašanja obavještajnih službi. Parlamentarni odbor za nadzor nad obavještajnim službama treba na povjerljivoj osnovi dobiti detaljnije i osjetljivije informacije na iste te teme. Te informacije moraju biti dovoljne da odbor na osnovu njih može adekvatno obavljati svoju funkciju nadzora. Ovo se detaljno treba propisati zakonom.

- Zakon koji regulira rad generalnog inspektora za obavještajne službe i/ili stručnog nadzornog tijela obavještajnih službi može propisati da tom organu i njegovim zaposlenima ne smije biti uskraćen pristup bilo kakvim obavještajnim podacima, informacijama ili prostorijama koje su pod kontrolom obavještajnih službi,te da svako uskraćivanje pristupa u tom smislu predstavlja krivično djelo.

- U krivičnim ili građanskim predmetima koji uključuju obavještajne službe, odluku o tome da li će se predmet u cjelini ili u dijelu pretresati iza zatvorenih vrata (in camera) donosi predsjedavajući sudija.

- Nadzorna tijela trebaju parlamentu podnositi jako važne izvještaje, a na svojim internet stranicama treba da objavljuju i svoje izvještaje, kao i izvještaje obavještajnih službi. Sljedeći koraci se mogu poduzeti kako bi se smanjili rizici da članovi parlamentarnog odbora za nadzor nad obavještajnim službama namjerno ili nenamjerno otkriju klasificirane informacije: članovi mogu proći sigurnosnu provjeru od strane obavještajne službe; mogu proći obuku o zaštiti klasificiranih informacija; a njihovi uredi, računari, telefoni i sistemi čuvanja dokumentacije mogu biti zaštićeni od prisluškivanja odnosno prismotre.

Bilješke

1. Ovo poglavlje se zasniva na mom iskustvu i istraživanjima kojima sam se bavio kao član Ministarske komisije za ocjenu rada obavještajnih službi (Ministerial Review Commission on Intelligence), koju je uspostavio ministar za obavještajne službe Južne Afrike 2006. god. Ono se zasniva i na publikaciji L. Nathan, *Lighting up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness*, Policy Paper (Birmingham, UK: Global Facilitation Network for Security Sector Reform, 2009).
2. Detaljnu raspravu o ovoj tački vidjeti u A. Wolfers, "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* Vol. 67, br. 4 (1952), str. 481–502.
3. Internet strana American Civil Liberties Union, *The Torture Report* (dostupno na www.thetorturereport.org).
4. *New York Times Co vs United States* 403 US 713 (1971) na 719.
5. *New York Times Co vs United States* 403 US 713 (1971).
6. Pogledati primjer takve ocjene rada u D. Banisar, "Public Oversight and National Security: Comparative Approaches to Freedom of Information," in *Democratic Control of Intelligence Services: Containing Rogue Elephants*, eds. H. Born and M. Caparini (Aldershot, UK: Ashgate, 2007), str. 217–235.
7. Informacije iz ovog okvira preuzete su iz Banisar, "Public Oversight."
8. Ovi izvještaji se mogu naći na internet stranici Holandske Generalne obavještajne i sigurnosne službe (dostupno na https://www.aivd.nl/english/). Izvještaj za 2010. vidjeti na https://www.aivd.nl/english/publications-press/@2827/annual-report-2010/.
9. Vidjeti internet stranicu kanadske sigurnosno-obavještajne službe (dostupno na www.csis-scrs.gc.ca).
10. Vidjeti Banisar, "Public Oversight."
11. Južna Afrika, Ministarska komisija za ocjenu rada obavještajnih službi (Ministerial Review Commission on Intelligence), *Obavještajne službe u ustavnoj demokratiji: Finalni izvještaj Ministru za obavještajnu službu, Časni g. Ronnie Kasrils, zastupnik) (Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP)* (10. septembar 2008) (dostupno na www.ssronline.org/document_result.cfm?id=3852).
12. Zakon o nadzoru nad obavještajnim službama Južne Afrike, Zakon br. 40 iz 1994, Čl. 4(2)(b).
13. C. Matei, "Romania's Transition to Democracy and the Role of the Press in Intelligence Reform," in Reforming Intelligence: Obstacles to Democratic Control and Effectiveness, uredn. T. Bruneau i S. Boraz (Austin: University of Texas Press, 2007), str. 227.
14. P. Gill, "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror,'" *Intelligence and National Security* Vol. 22, br. 1 (februar 2007), str. 14–37.
15. Potrebno je istaći raziku između generalnog inspektora za obavještajne službe koji je neovisno i zakonom uspostavljeno tijelo (kao što je slučaj u Australiji, Novom Zelandu i Južnoj Africi), i tijela koje je smješteno unutar obavještajne organizacije (kao što je slučaj kod Centralne obavještajne agencije (Central Intelligence Agency ili CIA) Sjedinjenih Država).
16. *Independent Newspapers (Pty) Ltd vs Minister for Intelligence Services* CCT 38/07 [2008] ZACC 6 (Južna Afrika).
17. Godišnji izvještaji Odbora mogu se naći na http://www.ctivd.nl/.
18. Za više informacija o sigurnosnoj provjeri članova parlamentarnih nadzornih odbora videti u H. Born i I. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005), str. 88–90.

POGLAVLJE 4

Provođenje nadzora

Monica den Boer

4

Provođenje nadzora

Monica den Boer

1. UVOD

U mladim demokratijama, učinkovit nadzor nad obavještajnom zajednicom je od velikog značaja zbog tenzije koja uvijek postoji između obavještajnog rada i određenih demokratskih vrijednosti, kao što su otvorenost i transparentnost. Ukoliko se državne obavještajne službe namjeravaju staviti pod vanjsku civilnu kontrolu, civili moraju biti podučeni o obavještajnom radu. U suprotnom će nad tim poslom i dalje monopol imati profesionalci iz službe. Također, treba razviti novu političku kulturu koja sprječava zloupotrebe obavještajnih službi dok istovremeno podržava njihovu legitimnu ulogu u demokratskom društvu.

U ovoom tekstu se objašnjava na koji način nadzorna tijela istražuju aktivnosti obavještajnih službi. Razmatra se najširi mogući spektar metoda nadzora, od *ad hoc* istraga do dugotrajnih istraživanja. Osim toga, uzima se u razmatranje i situacija kada više stalnih tijela imaju obaveze provođenja nadzora, i situacije kad ne postoje stalna tijela što iziskuje stvaranje privremenog tijela.

Dalje, namjera teksta je da posluži kao praktičan vodič kroz načine provođenja nadzora nad obavještajnim službama. Kako su nadzorna tijela u različitim zemljama suočena sa mnogim sličnim izazovima, razumijevanje osnovne metodologije može pomoći novim nadzornim tijelima da izbjegnu najčešće zamke i uvećaju svoju učinkovitost.

2. RAZLOZI ZA PROVOĐENJE NADZORA NAD OBAVJEŠTAJNIM SLUŽBAMA

Odgovornost obavještajnih službi ima više dimenzija. Neke od njih se odnose na kontrolu obavještajnih službi iznutra, od strane zvaničnika iz službe, i spolja, od strane izvršne vlasti. Druge se odnose na nadzor koji vrši parlament, sudstvo i stručna nadzorna tijela (vidjeti Born i Geisler – Poglavlje 1). Temeljna svrha nadzora nad obavještajnim službama je odvraćanje domaće obavještajne službe od nepravilnog rada. Za razliku od *kontrole*, koja se odnosi na direktno upravljanje službom, *nadzor* obuhvaća monitoring, evaluaciju, detaljni pregled i ocjenu rada. Promoviranjem otvorenosti i transparentnosti, nadzorna tijela mogu spriječiti širenje tendencija zloupotrebe u službi i pružiti parlamentarnim zastupnicima i izvršnoj vlasti (kao i drugima koji su nadležni za provođenje kontrole) korisne informacije i stručnost.

2.1 KRŠENJA LJUDSKIH PRAVA

Moguće kršenje ljudskih prava od strane obavještajnih službi je uvijek razlog za zabrinutost javnosti. Tokom 1960-ih i 1970-ih, na primjer, agencije vlade SAD su odobrile agresivne tajne obavještajne operacije protiv pokreta za građanskih prava i antiratnih pokreta. U nešto skorijoj prošlosti, državne obavještajne službe koje sarađuju u borbi protiv terorizma pribjegavala su nezakonitom izručenju (eng. extraordinary rendition) osoba, vodile su tajne centre za pritvor, te su informacije od osumnjičenih izvlačile mučenjem. Ovakva sredstva, koja otvoreno krše ljudska prava, su neka od pitanja koja potpadaju pod nadzor.

Na nedolične i/ili nezakonite aktivnosti pažnju nadzornim tijelima često skreću mediji, posebno novinari koji se bave istražiteljskim novinarstvom na osnovu informacija dobivenih od nevladinih organizacija kao što su „Human Rights Watch“ i „Amnesty International“. Prema Marini Caparini,

> *„Mediji čine vezivno tkivo koje povezuje pojedince i grupe sa vladom i igraju kritičnu ulogu u prenošenju informacija o promjeni javnog mišljenja i političkim preferencama. Javnost se informira prvenstveno preko slobodne štampe, a mogućnost uvida javnosti u vladine odluke, radnje i eventualne zloupotrebe podseća vladu da treba da bude odgovorna.“*[1]

2.2 PARLAMENTARNA PITANJA

Zastupnici u nacionalnim parlamentima, čak i oni koji nisu članovi nadzornih odbora, mogu pokrenuti pitanja vezana za djelovanje obavještajnih službi. Ona se mogu kretati od općih pitanja o nivou prijetnji i prioriteta službi do konkretnih pitanja koja se odnose na metode tajnog prikupljanja podataka i veza sa određenim grupama. Ponekad ova pitanja mogu ukazati na pravne praznine koje se pojavljuju kada se pokrenu nove operacije za koje još ne postoje mehanizmi nadzora. Na primjer, 2003. godine, holandski parlamentarni zastupnici su postavili pitanja vezano za prikupljanje obavještajnih podataka u pogledu oružja masovnog uništenja kojeg je navodno posjedovala bivša vlada Sadama Huseina u Iraku.[2] Ta su pitanja dovela do osnivanja Holandskog istražnog odbora za Irak (Dutch Committee of Inquiry on Iraq).

3. MANDATI ZA NADZOR

Obavještajne službe se moraju pridržavati zakona, direktiva, naloga i politika vlade kojoj služe.[3] Isto tako, nadzorna tijela za obavještajne službe se moraju pridržavati zakona odnosno mandata koji istovremeno uspostavlja i ograničava njihova istražna ovlaštenja. Mandat za nadzor se često formulira na najneutralniji mogući način kako bi se izbjegla politička sporenja. Ovo je od posebnog značaja kada je nadzorno tijelo privremenog karaktera, kao što je to slučaj sa *ad hoc* istragom nekog konkretnog incidenta. Ipak, mandati trebaju biti konkretni, jasni i razmjerni ovlaštenjima, metodama i resursima službe odnosno službi čiji nadzor vrše.

Mandati nadzornih tijela mogu biti komplementarni, ili se mogu preklapati. Poželjnija je ova druga varijanta, pošto se samo jedan mehanizam nadzora generalno smatra nedovoljnim. Iz tog razloga, sistem obavještajnog nadzora u Italiji je nedavno proširen, i umjesto čistog naknadnog (ex post) nadzora od strane Ustavnog suda, sada postoje dva nova mehanizma: interno administrativno tijelo (Ured generalnog inspektora) i tijela vanjske politike (Parlamentarni odbor za sigurnost Republike [COPASIR]).[4] Kanadska sigurnosno-obavještajna služba (Canadian Security Intelligence Service -CSIS) ima četiri nadzorna mehanizma čije se nadležnosti međusobno preklapaju: Generalni inspektor, koji prati poštivanje operativnih politika od strane CSIS-a; Odbor za ocjenu rada sigurnosno-obavještajne službe (Security Intelligence Review Committee - SIRC), koji ocjenjuje aktivnosti CSIS-a i istražuje žalbe na ovu službu (vidjeti Farson – Poglavlje 2); Savezni sud Kanade, koji je jedino tijelo ovlašteno da odobrava korištenje posebnih istražnih radnji;[5] i javno izvještavanje, u obliku godišnje izjave ministra javne sigurnosti o državnoj sigurnosti i Javnog izvještaja CSIS-a.[6]

Mandat parlamentarnog nadzornog odbora kao što je COPASIR bi trebalo obuhvatiti cjelokupnu obavještajnu zajednicu zemlje, uključujući i odjele i zvaničnike koji im pružaju podršku.[7] Odbor treba imati sva ovlaštenja koja mu trebaju da može pratiti zakonitost, efikasnost i učinkovitost obavještajnih službi, kao i njihove budžete i računovodstvene prakse, poštivanje standarda ljudskih prava i druge administrativne/političke aspekte. Kada odboru mandat ne omogućuje da radi navedeno, taj mandat treba revidirati. Na primjer, kada je jedna *ad hoc* istraga u Australiji pokazala da Organizacija za obrambeno geoprostorno snimanje (Defence Imagery and Geospatial Organization - DIGO) nije dovoljno odgovorna za svoj rad zbog ograničenosti mandata nadzornih tijele, istraga je preporučila da se mandat odgovarajućeg parlamentarnog odbora proširi kako bi obuhvatio sve obavještajne službe Australije. Istraga je također preporučila da se mandat Generalnog inspektora za obavještajne i sigurnosne službe (Inspector General of Intelligence and Security) proširi kako bi obuhvatio monitoring DIGO-a (vidjeti Born i Geisler– Poglavlje 1).[8]

3.1 VRSTE MANDATA

Mandati mogu biti široki i uski. Na primjer, mandat jednog nadzornog tijela može biti da provjerava zakonitost rada samo jedne obavještajne službe. Istovremeno, neko drugo tijelo može imati zadatak da ocjenjuje učinkovitost više agencija, uključujući rad zaposlenih u njima i provođenje budžetskih procesa. Širi mandati generalno pomažu da se izbjegne iscjepkanost ili druge negativne posljedice usko postavljenog nadzora.

Mandat za nadzor ponekad obuhvaća ovlaštenja koja se protežu i izvan onih koja su strogo neophodna za provođenje monitoringa. Na primjer, mogu obuhvatiti ovlaštenja

za hapšenje i pritvor, kao i korištenje sile. Mogu, također, obuhvatiti kontrolu prijenosa informacija stranim službama i odobrenje imenovanja na najviše izvršne pozicije u obavještajnim službama.[9]

Što se tiče tajnih aktivnosti, posebno onih gdje se koriste posebne istražne radnje za prikupljanje osobnih podataka, mandati nadzora katkad uključuju preventivne ili proaktivne ovlasti. Na primjer, u Belgiji, Zakon o posebnim obavještajnim službama (Special Intelligence Act) daje pravo Stalnom odboru za ocjenu rada obavještajnih agencija (Standing Intelligence Agencies Review Committee) (Odbor I —stručno nadzorno tijelo) da daje mišljenje službama o korištenju posebnih istražnih radnji. Ako je njegovo mišljenje negativno, službe se ne mogu žaliti. Nadalje, ukoliko Stalni odbor utvrdi postojanje nezakonitih radnji tokom provođenja monitoringa korištenja posebnih istražnih radnji, on iste može suspendirati.[10]

Mandati nadzora mogu također uključiti i detaljno praćenje budžeta. U UK, na primjer, računovodstvo obavještajne službe podliježe reviziji Državnog ureda za reviziju (National Audit Office), a također i pažljivom ispitivanju od strane parlamentarnog Odbora za obavještajne i sigurnosne službe (Intelligence and Security Committee), u čijem se godišnjem izvještaju objavljuju neki detalji finansiranja i rashoda obavještajne službe.[11] Isto tako, Južnoafrički zajednički odbor za obavještajne službe (South African Joint Committee on Intelligence) pažljivo ispituje finansijsko upravljanje u obavještajnim službama te zemlje,[12] dok u Poljskoj parlamentarni nadzorni odbor razmatra nacrt budžeta za obavještajne službe i prati njegovu realizaciju. Neke države idu čak tako daleko da kontrolu budžeta uključe u mandat svojih nadzornih tijela. Na primjer, Argentinski dvodomni odbor za nadzor nad obavještajnim tijelima i aktivnostima (Argentinean Bicameral Committee for the Oversight of Intelligence Bodies and Activities) i Kongresni odbori za obavještajne službe SAD-a (the US congressional intelligence committees) raspolažu takvim ovlaštenjima.

3.2 IZMJENE MANDATA

Mandati nadzornih tijela za obavještajne službe ne moraju biti fiksni. Na primjer, kada se proširi mandat obavještajne službe, također je potrebno revidirati i mandat tijela koje nadzire njeno djelovanje.[13]

Strateški događaji koji imaju značajne političke posljedice također mogu inicirati promjene mandata nadzornih tijela za obavještajne službe, posebno kada je došlo do propusta u radu obavještajne službe. Na primjer, propust obavještajnih službi SAD-a da otkriju i spriječe napade 11. septembra doveli su do razmatranja cjelokupnog mehanizma razmjene obavještajnih informacija. Promjene tih mehanizama utjecale su na rad nadzornih tijela, te su dovele do promjene i njihovih mandata.

Neki put nadzorna tijela, tokom obavljanja svoga posla, i sama mogu utvrditi koje je promjene potrebno izvršiti u njihovim mandatima. Iz tog razloga neka nadzorna tijela vrše redovne strateške ocjene sa ciljem utvrđivanja i davanja preporuke o takvim promjenama. Na ovaj način nadzorna tijela mogu nedostatke pretvoriti u pozitivne, konstruktivne preporuke u cilju unaprjeđenja obavještajnog sektora.

4. OVLAŠTENJA ZA PROVOĐENJE NADZORA

Ovlaštenja koja se daju nadzornim tijelima za obavještajne službe mogu biti međusobno vrlo različita. Ona koja se navode dalje u tekstu se smatraju najuobičajenijima. Svakako, ova lista nije potpuna. Na primjer, neki mandati podrazumijevaju ovlaštenje za upućivanje, čime se daje pravo nadzornom tijelu da uputi neki nalaz o nepravilnostima u radu nekom unutarnjem tijelu (kao što je generalni inspektor) za pokretanje disciplinskog postupka, ili vanjskom tijelu, za pokretanje krivičnog postupka. Ovlaštenje razotkrivanja je ovlaštenje nadzornih tijela da razotkriju nepridržavanje pravila i propisa, greške u procjenama, ili povrede zakona najvišem organu relevantne države, kao što je Državni pravobranitelj (Attorney General) u Sjedinjenim Državama – što je više od prijavljivanja generalnom inspektoru.

4.1 PRAVO NA INFORMIRANOST

Pravo na informiranost, koje daje nadzornim tijelima pristup informacijama, može biti pasivno ili aktivno. Nadzorno tijelo koje ima pasivno pravo na informiranost može dobivati informacije o obavještajnim aktivnostima u obliku dokumenata i rezimea (eng. briefings). Idealno bi bilo da su ti rezimei aktualni i sveobuhvatni. Ali, u zavisnosti od važećih zakona, oni ne moraju nužno uključivati visoko osjetljive informacije kao što su budžetska pitanja i tajne operacije.

Nadzorna tijela koja imaju samo pasivno pravo informiranost su potpuno ovisna o agencijama koje nadziru u smislu obima i preciznosti informacija koje dobivaju. Iz tog razloga, poželjno je da nadzorna tijela imaju i pasivna i aktivna prava informiranja. Nadzorna tijela koja imaju aktivno pravo informiranja mogu tražiti informacije koje im trebaju. Na primjer, tako što prinude zvaničnike da pruže informacije ili dođu u nenajavljeni obilazak prostorija službe.

Iako nadzorna tijela treba da imaju neograničen pristup svim informacijama koja su im potrebna da bi mogla obavljati svoju dužnost, to nije uvijek slučaj. Na primjer, većina nadzornih tijela ima pristup povjerljivim informacijama, ali ima ih koja nemaju. S druge strane, neka ograničenja mogu biti opravdana, kao npr. ona koja štite identitet izvora. Takva se ograničenja, na primjer, odnose na pristup informacijama južnoafričkog parlamentarnog Zajedničkog stalnog odbora za obavještajne službe (Joint Standing Committee on Intelligence). U Argentini, Kanadi i Sjedinjenim Državama, određena nadzorna tijela imaju neograničen pristup informacijama.

4.2 ISTRAŽNA OVLAŠTENJA

Osim čiste mogućnosti da pažljivo istraže informacije koje im se dostavljaju, nadzorna tijela za obavještajne službe treba da imaju pravo pokretanja istraga. Holandski odbor za ocjenu rada obavještajnih i sigurnosnih službi (CTIVD), na primjer, ima pravo pokretanja istraga na osnovu žalbi koje su mu podnesene vezano za rad obavještajnih službi. Mandati drugih nadzornih tijela daju im pravo da sama pokreću istrage, bez konkretne pritužbe koja će poslužiti kao osnova za to. Određene istražne ovlasti uključuju pravo da se zahtijeva i/ili obavežu zvaničnici da se pojave pred nadzornim tijelom da bi odgovorili na pitanja.

4.3 PRAVO ODOBRAVANJA

Neki mandati daju nadzornim tijelima pravo da odobravaju odnosno usvajaju strateške obavještajne programe, budžete službe, kao i imenovanja na najviše pozicije u obavještajnim službama. Nadzorna tijela koja posjeduju jedno ili više ovih ovlaštenja za odobravanje mogu ih koristiti da izvrše značajan utjecaj na službu koju nadziru, posebno kad se radi o određivanju obavještajnih prioriteta. Na primjer, „moć novčanika" koju imaju kongresni obavještajni odbori u SAD smatra se snažnim instrumentom nadzora i kontrole, jer omogućava odborima da pokažu koji su obavještajni i politički prioriteti kroz izdvajanja sredstava.

5. METODE NADZORA

Osim definiranja ovlaštenja, mandat nadzornog tijela treba definirati metode koje ono može koristiti pri provođenju istraga. Metode koje se najčešće koriste su inspekcije, saslušanja i analiza dokumenata. Osim toga, tu su intervjui, izjave svjedoka i direktni pristup bazama podataka (ovo posljednje belgijski i holandski zvaničnici smatraju ključnim metodom nadzora). Sve ove metode se koriste pojedinačno, zajednički, i jedna za drugom u cilju ostvarivanja ciljeva nadzora.

5.1 INSPEKCIJE

Neka nadzorna tijela vrše redovne inspekcije prostorija obavještajnih službi koje nadziru. Te inspekcije se mogu vršiti na godišnjem, kvartalnom ili čak mjesečnom nivou. U većini slučajeva, nadzorna tijela informiraju obavještajne službe o svojim posjetama, ali mnoge imaju i pravo doći u nenajavljene inspekcije. Tokom tih posjeta, članovi nadzornih tijela mogu razgovarati sa zaposlenima ili ući u kompjuterske baze podataka koristeći pri tom tehnike poput nasumičnog uzorka. U Norveškoj, parlamentarni odbor za nadzor nad obavještajnim službama (poznat pod nazivom EOS odbor) vrši nekoliko inspekcija svake godine, a u Holandiji CTIVD ima sličan mandat. Na Novom Zelandu, Generalni inspektor za obavještajne i sigurnosne službe ima ovlaštenje da uđe u prostorije službe, ali samo uz prethodnu najavu direktoru službe.[14]

5.2 SASLUŠANJA

Saslušanja su uobičajen način na koji nadzorna tijela dolaze do informacija od osoba zaposlenih u obavještajnim službama, neovisnih stručnjaka i drugih ispitanika. Iako su saslušanja teška i osjetljiva, mogu biti od suštinskog značaja u pružanju dodatnih objašnjenja situacijama za koje je osobena slaba ili nedostatna dokumentacija. Saslušanja, također, mogu pomoći u raspodjeli političke i/ili odgovornosti u okviru izvršne vlasti za odluke koje su donijeli ili primijenili obavještajni ili drugi zvaničnici. Istraga koja se trenutno vodi u Ujedinjenom Kraljevstvu o uključenosti ove zemlje u rat u Iraku, kojom predsjedava Sir John Chilcot, održala je brojna javna saslušanja, koja su sva prenošena u realnom vremenu.[15] Holandski odbor za istragu o Iraku održao je slična saslušanja, s tom razlikom da ona nisu bila javna.

5.3 ANALIZA DOKUMENTACIJE

Nadzorna tijela redovno razmatraju klasificirane i neklasificirane izvještaje i drugu

dokumentaciju koju dostavljaju obavještajne službe. Ta dokumentacija često sadrži korisne informacije i može dati odgovore na neka pitanja. Ali, mogu se pojaviti i druga pitanja koja se odnose na rad obavještajne službe na koja se odgovori moraju naći na drugi način.

Analiza dokumentacije se ne treba ograničavati na dokumentaciju koju izrađuju obavještajne službe. Holandski odbor za istragu o Iraku, na primjer, napravio je javnu internet stranicu preko koje je pozivao na dostavljanje druge dokumentacije koja bi mogla biti od koristi.

6. VRIJEME ZA PROVOĐENJE NADZORA

Nadzor se može odvijati prije nego što se donese odluka o nekoj operaciji ili politici, tokom njene realizacije, ili nakon njenog završetka. Vrijeme nadzora zavisi od mandata nadzornog tijela

6.1 NAKNADNI (*EX POST*) NADZOR

Najčešći oblik nadzora je *ex post* nadzor. Objašnjenje za to se nalazi u argumentu da nadzorna tijela trebaju ocjenjivati, ali se ne trebaju miješati u odluke rukovodstva obavještajne službe.[16] *Ex post* nadzor ne isključuje obavještavanje nadzornih tijela o planiranim ili tekućim operacijama, ali snažno implicira da će nadzorno tijelo razmatrati događaje u retrospektivi i staviti pod lupu samo one koji su se već desili.

6.2 PRETHODNI (*EX ANTE*) NADZOR

Neka nadzorna tijela imaju mandat da rade nadzor *ex ante*. Nadzor *ex ante* se smatra načinom da se unaprijedi autoritet nadzornog sistema. To podrazumjeva inspekciju i/ili odobrenje obavještajnih radnji prije nego što se one izvrše. Također, može se govoriti o „proaktivnom mandatu“ koji se definira kao „mandat koji omogućuje nadzornom tijelu da uloži veto ili da promijeni politiku ili funkcioniranje službe prije nego što se neka politika ili operacija realizira.“[17] Mnoga nadzorna tijela su u poziciji da pažljivo proučavaju politiku i strategiju relevantnih obavještajnih službi i mogu zatražiti ili naložiti internim tijelima za ocjenu rada da provedu istragu prije započinjanja određene obavještajne radnje ili tajne operacije.

Specijalni izvjestilac UN-a za promociju i zaštiti ljudskih prava i sloboda u borbi protiv terorizma (Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism) preporučuje nadzor *ex ante*, kojega smatra korisnim za sprječavanje kršenja ljudskih prava od strane obavještajnih službi u borbi protiv terorizma. Isto tako, preporučuje se da nadzorna tijela vrše *ex ante* ocjenu sporazuma o saradnji između domaćih obavještajnih službi i stranih partnera prije potpisivanja tih sporazuma (vidjeti Roach – Poglavlje 7).[18]

S druge strane, nadzorna tijela koja vrše *ex ante* ocjenu mogu se ponekad smatrati odgovornim za neuspjehe obavještajne službe i povrede zakona do kojih dođe zbog odobrenih aktivnosti. Mogućnost nadzornog tijela da vrši *ex ante* ocjenu također može negativno utjecati na odnose sa partnerskim službama iz inostranstva koje više vole da ne otkrivaju povjerljive informacije nadzornim tijelima.[19]

Mnoge domaće obavještajne službe dijele sličnu sigurnosnu zabrinutost u pogledu otkrivanja unaprijed informacija o operacijama, posebno kada su u to uključeni zastupnici u parlamentu. Iz tog razloga, zastupnici koji su članovi nadzornih odbora nad obavještajnim službama često moraju proći kroz detaljan postupak sigurnosne provjere. No, ponekad se čak ni ova mjera opreza ne smatra dovoljnom.

6.3 PERIODIČNI NADZOR

Nadzor se također može vršiti periodično. Mandati obavještajnih službi često iziskuju da visoko rukovodstvo izrađuje redovne (obično godišnje) izvještaje o aktivnostima službe koje podnosi izvršnoj vlasti, parlamentu, ili oboma. Isto tako, nadzorna tijela mogu detaljan nadzor vršiti ciklično, umjesto epizodno. Svjestan ograničenosti svojih kapaciteta, kanadski SIRC usvaja plan koji predviđa nadzor svih aspekata obavještajnih službi u ciklusu od tri do pet godina. Izvještaj *ad hoc* istrage obavještajne službe Australije (o kojemu je prethodno u tekstu bilo riječi) isto tako preporučuje da se ocjena obavještajne zajednice vrši svakih pet do sedam godina.[20]

7. ISTRAGE VEZANE ZA NADZOR

Istrage se mogu pokrenuti na više različitih načina. Jedan od njih je na zahtjev parlamentarnih zastupnika ili predstavnika izvršne vlasti. Mogu ih pokrenuti i mediji. U pojedinim zemljama, poput Belgije ili Kanade, pritužba koju uloži pojedinac pokreće istragu. Često, nadzorna tijela imaju ovlaštenje i da pokrenu vlastite istrage. Ipak, u većini slučajeva, nadzorna tijela imaju pravo konačnog odlučivanja o pokretanju neke istrage.

7.1 ISTRAGA KONKRETNIH SLUČAJEVA

Nadzorno tijelo može pokrenuti istrage konkretnih slučajeva na osnovu navoda koje dostavi, na primjer, osoba koja se žali, parlamentarni zastupnik, ili mediji. Tijelo za nadzor može, također, pokrenuti ovakve istrage i na svoju sopstvenu inicijativu. U skladu sa odgovarajućim procedurama, obavještajne službe mogu dostaviti nadzornom tijelu izvještaje o ozbiljnim događajima, koji se mogu odnositi, na primjer, na nezakonite aktivnosti, slučajeve ugrožavanja sigurnosti, ili curenje informacija. Ovi se izvještaji mogu dostavljati bilo na redovnoj osnovi, bilo u okviru *ad hoc* istraga. Jedan takav izvještaj je pripremila Kraljevska kanadska konjička policija (Royal Canadian Mounted Police - RCMP), odnosno Kanadska komisija za istraživanje radnji kanadskih zvaničnika u vezi sa slučajem Maher Arar (Canadian Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar). Ovom istragom je, između ostalog, utvrđeno da RCMP nije ispoštovao vlastite politike vezane za provjeru osobnih podataka u smislu relevantnosti i pouzdanosti prije nego što ih je dostavio drugim obavještajnim službama. Među dvadeset tri preporuke koje je dala ova Komisija, bilo je i upozorenje da se RCMP treba zadržati u okviru svog mandata policijske snage.[21]

7.2 TEMATSKE ISTRAGE

Tematske istrage se fokusiraju na šira pitanja, a ne na određene događaje. Ponekad proisteknu iz razmatranja konkretnih događaja, koja na kraju otkriju mnogo dalekosežnije probleme.

Okvir 1: Holandska parlamentarna istraga posebnih istražnih radnji: studija slučaja tematskog nadzora

Jedan holandski međuregionalni krivični istražni tim, kojemu je dato u zadatak da prikupi obavještajne podatke o jednom krijumčaru droge, je 1993. godine koristio posebne istražne mjere u provođenju tog svog zadatka. Navodno, te su mjere uključivale i nezakonite radnje, posebno kontrolirano puštanje droge na tržište. Kao odgovor na navodne nepravilnosti, ovaj je tim rasformiran, i, u aprilu 1994. godine, holandski je Parlament pokrenuo formalnu istragu korištenja posebnih istražnih radnji od strane holandskih vlasti.[22]

Istraga je započela analizom dokumentacije i orijentacijskim razgovorima sa političarima i obavještajcima. Osim toga, istraga je angažirala naučne radnike da izrade dva izvještaja: procjenu prirode, ozbiljnosti i obima organiziranog kriminala u Holandiji i komparativnu međunarodnu studiju zakonodavstva kojim se regulira korištenje posebnih istražnih radnji.

U međuvremenu, osoblje angažirano da vrši istragu (od kojih je svaki pojedinac bio predmet sigurnosne provjere) sprovodilo je zatvorena saslušanja tokom šest mjeseci. Svrha tih saslušanja bila je da se prikupe informacije i ostvari uvid u korištenje posebnih istražnih radnji u Holandiji. Zatvorena saslušanja su također služila kao priprema za seriju otvorenih, javnih saslušanja koja su direktno prenošena.

Ova istraga, koja je okončana 1996. godine, rezultirala je detaljnim izvještajem na 6.700 strana i sa 129 preporuka. Dvije godine kasnije, Parlament je osnovao novi, privremeni odbor, čiji je zadatak bio da izvrši procjenu primjene ovih preporuka. Novi odbor je došao do velikog broja novih informacija, uključujući i dokaze o korupciji vezanoj za drogu u policijskim i carinskim službama. Ova otkrića su gotovo prinudila ministra pravosuđa, Benka Korthalsa, da podnese ostavku na svoju funkciju, ali je on ipak uspio preživjeti parlamentarnu raspravu.

8. ORGANIZACIJA NADZORA

Pošto je najučinkovitiji nadzor onaj koji je sistematičan, poželjno je podijeliti proces nadzora u odvojene faze koja slijede jedna drugu.

8.1 IDENTIFIKACIJA I ODABIR PITANJA

Obavještajni rad je kompleksno, dinamično polje na kojem djeluje više aktera, procedura i politika. Iz tog razloga, veliki broj pitanja postaje predmetom nadzora obavještajnih službi. Najbolji način za započinjanje procesa nadzora jeste da se napravi popis svih mogućih pitanja, te da se onda uporedi sa zakonskim mandatom nadzornog tijela. Područja gdje se utvrde poklapanja ukazuju na odgovarajuća pitanja koja mogu postati predmetom detaljnog nadzora.

8.2 DOBIVANJE SIGURNOSNIH ODOBRENJA

Pripadnici i zaposlenici nadzornih tijela generalno trebaju dobiti sigurnosna odobrenja da bi mogli raditi sa povjerljivim informacijama. Izuzeci koji se ovdje trebaju spomenuti su pripadnici parlamentarnih nadzornih odbora, koji se često protive istragama svoga osobnog života, posebno kada su obavještajne službe koje vrše te sigurnosne provjere upravo ono tijelo koje je podvrgnuto njihovoj ocjeni ili istrazi, što je paradoks. Ipak, izuzimanje političara od sigurnosnih provjera je vrlo kontroverzno pitanje.

8.3 OSIGURANJE PROSTORIJA NADZORNOG TIJELA

Prostorije nadzornog tijela trebaju biti sigurne. Na primjer, redovno se treba provjeravati da li su postavljeni elektronski prislušni uređaji. Osim toga, kompjuteri i druge naprave informacijske tehnologije treba da budu šifrirani i zaštićeni lozinkama. Isto tako, cjelokupno prateće osoblje koje ima pristup prostorijama (uključujući sekretare, prevodioce, ugostitelje i čistače) treba proći sigurnosne provjere.

8.4 OSIGURANJE DOKUMENTACIJE I DRUGOG MATERIJALA

Članovi nadzornih tijela moraju biti disciplinirani u rukovanju dokumentima i bilješkama. Neophodno je pridržavati se politike „čistog stola“, koji podrazumijeva da se povjerljive informacije rutinski pohranjuju u sef. Povjerljivi dokumenti, bilo odštampani na papiru ili u digitalnom obliku na kompjuteru ili memorijskom drajvu, nikada ne smiju napustiti ured bez odgovarajućih odobrenja. Interna evidencija koja se odnosi na povjerljive izvore, svjedoke i duge ključne ispitanike se treba voditi anonimno. I na kraju, svi ovi uslovi se trebaju izričito navesti u internom priručniku o pravilima službe.

8.5 IZRADA PLANA

Od pojedinih nadzornih tijela se traži da pripreme skup propisa ili protokola, ili čak detaljnih planova inspekcije, i da dobiju odobrenje za njih prije nego što započnu bilo kakve aktivnosti nadzora. Svrha ovoga je da se izbjegnu nesporazumi vezani za prava i ovlaštenja nadzornog tijela, te prava i ovlaštenja obavještajnih službi koje su podvrgnute nadzoru. U ovim dokumentima se kao minimum navodi identitet odeljenja ili obavještajne operacije koja se provjerava, kao i dokumenta koja će biti podvrgnuta detaljnom preispitivanju, te tehnologije koje će se pri tome koristiti.

S obzirom da nadzor može biti složen, obično je od koristi članovima nadzornog tijela, čak i kada to nije posebno propisano, da izrade i usvoje zajednički scenarij prije nego što započnu aktivnosti nadzora. Detaljni planovi inspekcije, prije svega, potiču posvećenost procesu nadzora različitih aktera koji su u nju uključeni. Nadalje, izrada detaljne procedure unaprijed olakšava pripadnicima nadzornog tijela da se koncentriraju na sadržaj kada inspekcija počne.

Okvir 2: Elementi osnovnog plana inspekcije

- datum inspekcije;
- zakonska osnova za provođenje inspekcije;
- svrha inspekcije;
- zadaci inspekcije;
- imena nadzornog osoblja koje vrši inspekciju;
- identifikacija odjeljenja službe koje je predmet istrage;
- imena osoba iz službe sa kojima će se obaviti razgovori;
- zahtjevi za razgovore;
- lista dokumenata koji će se pregledati;
- predinspekcijski zahtjev za dokumentacijom;
- resursi;
- administrativna pomoć;
- rokovi izvještavanja.[23]

Okvir 3: Dopunski zadaci koji se postavljaju pred detaljni plan inspekcije

- Odrediti rokove za različite aktivnosti inspekcije;
- Napraviti listu osoba sa kojima će se obaviti razgovori;
- Pisanje pozivnog pisma potencijalnim ispitanicima, kao i pisma zahtjeva nadređenima tih ispitanika za čije je svjedočenje potrebno dobiti dozvolu;
- Izrada protokola za rad sa ispitanicima koji imaju diplomatski status (privilegije i imunitet).
- Odluka o vrstama razgovora koji će se voditi (povjerljivi, anonimni, snimani, itd.)
- Izrada protokola za vođenje intervjua u kojem će se riješiti pitanja poput: Hoće li se ispitaniku pitanja dostaviti unaprijed? Hoće li se ispitaniku dopustiti da koristi dokumentaciju ili nešto drugo što će mu pomoći u prisjećanju tokom razgovora? Ima li ispitanik pravo da pogleda ili korigira transkript razgovora?
- Izrada protokola za rad sa povjerljivim izvorima i informacijama;
- Dogovaranje pomoći za transkripciju i prevođenje;
- Izrada protokola za objavljivanje informacija do kojih se dođe tokom razgovora.

9. PROFESIONALIZAM I VJERODOSTOJNOST NADZORNIH TIJELA

Ljudi koje žive u demokratskim državama očekuju od vladinih agencija svoje zemlje da se pridržavaju zakona te zemlje i, u slučaju da to ne čine, da budu pozvane na odgovornost od strane nadzornih tijela. Zbog posebnih ovlaštenja koje posjeduju obavještajne službe – da mogu ograničiti ili prekršiti ljudska prava – tijela koja nadziru te službe imaju povećanu

odgovornost. Stoga je na njima da pokažu prilikom vršenja nadzora i ponašanju u javnosti najviše profesionalne standarde. U suprotnom, kredibilitet nadzornog procesa će trpjeti negativne posljedice i javnost će izgubiti povjerenje u institucije svoje vlade.

9.1 NEOVISNOST NADZORNOG TIJELA

Nadzorno tijelo se ne može smatrati profesionalnim ukoliko njegova neovisnost i autonomija nisu apsolutno garantirane zakonom. Profesionalizam također iziskuje da nadzorna tijela budu potpuno nestranačka – to jest, bez pritisaka stranačke politike, miješanja izvršne vlasti i pritiska medija.

U praktičnom smislu, najbolji način odbrane od političkih ili medijskih pritisaka je da ih se bude svjestan. Iz tog razloga, osoblje nadzora često ima koristi od obuke u radu s medijima, što ih, između ostalog, priprema da pruže odgovor na neočekivana pitanja političara ili medija. Ovo je posebno važno u svjetlu potrebe da se spriječi nenamjerno otkrivanje povjerljivih informacija kada se odgovara na takva pitanja.

9.2 STRUČNOST NADZORNOG OSOBLJA

Idealno bi bilo da pripadnici nadzornih tijela i njihovi zaposlenici posjeduju znanje i iskustvo u radu sa nizom sigurnosnih agencija, uključujući policiju i vojne agencije, kao i strane i domaće obavještajne službe. Oni koji to iskustvo ne posjeduju trebaju proći obuku što je prije moguće, i treba ih se ohrabrivati i/ili od njih zahtijevati da redovno pohađaju obrazovne seminare i obuke, kao i da revidiraju odnosna pravila i propise.

9.3 POVJERLJIVE INFORMACIJE

Jedna od najtežih profesionalnih dilema sa kojom se suočavaju zaposleni jeste kako uspostaviti ravnotežu između međusobno suprotstavljenih zahtjeva za transparentnošću i tajnošću (vidjeti Nathan – Poglavlje 3). S obzirom da otkrivanje određenih povjerljivih informacija stvarno može dovesti nacionalnu sigurnost u opasnost, vlade imaju legitimno pravo da takve informacije ne daju javnosti. Upravo iz tog razloga, zaposlenici u nadzornim tijelima moraju prvo proći sigurnosne povjere prije nego što mognu raditi sa povjerljivim informacijama. Ipak, pretjerana tajnovitost je jednako nepoželjna, posebno kada se pretjera u klasificiranju informacija kao povjerljivih kako bi se prikrile radnje koje bi mogle imati politički neželjene posljedice (kao što je, na primjer u SAD-u, postojanje tajnih programa lišavanja slobode, ispitivanja i nezakonito izručenja osoba drugim zemljama). Zloupotreba zakona o tajnosti države može dovesti do toga da građani izgube povjerenje u svoju vladu, čime se podriva legitimitet svih vladinih institucija. Nadalje, pretjerana povjerljivost ugrožava učinkovitost nadzora. Ovaj se problem u nekim državama ublažava zakonima koji omogućuju sudstvu da utvrdi da li je neki dokument pravilno klasificiran.

10. PRINCIPI RADA NADZORNIH TIJELA

Sam način na koji nadzorno tijelo obavlja svoje poslove može imati značajan utjecaj na njegovu učinkovitost. Ukoliko nadzorna tijela sama ne poštuju vrijednosti poput transparentnosti i dosljednosti, ne mogu legitimno očekivati od obavještajnih službi da učine to isto.

10.1 TRANSPARENTNOST

Učinkovitost nadzornog tijela se najbolje postiže njihovom maksimalnom transparentnošću. Posebno je od velikog značaja da nadzorna tijela djeluju u skladu sa dogovorenim standardima i protokolima, kako bi uvijek mogli objasniti svoje radnje i demonstrirati istu odgovornost koju očekuju od obavještajnih službi koju nadziru. Nadzorna tijela mogu dodatno unaprijediti transparentnost rada tako što će u svoje izvještaje uključiti informacije o izvorima sa kojima su obavljene konsultacije i opis zadatka korišten za konkretnu istragu.

10.2 DOSLJEDNOST

Skandali obično dovedu do naglog skoka u nadzoru nad obavještajnim službama, nakon čega uslijede periodi rigoroznog monitoringa. Ipak, važno je da se nadzor odvija na tekućoj osnovi, a ne samo kao odgovor na probleme kada se oni pojave na površini. Nadzorna tijela za obavještajne službe mogu promovirati veću dosljednost u svom radu tako što će razviti obrasce monitoringa i inspekcija. Takvim pristupom se pomaže izbjegavanje nepažnje ili pojave novih praznina u nadzoru, i u konačnici smanjuje vjerojatnost ponavljanja propusta obavještajne službe.

10.3 SARADNJA SA OBAVJEŠTAJNIM SLUŽBAMA

Iako se obavještajne službe mogu činiti zatvorenim, izoliranim birokratijama, u većini se slučajeva radi o savjesnim organizacijama koje su spremne ispravljati vlastite nedostatke. Iz tog razloga, u interesu je nadzornih tijela da u interakciji sa obavještajnim službama djeluju angažirano, pravovremeno i instruktivno. Na primjer, određene preporuke za provođenje korektivnih radnji treba da se predstave na način koji će omogućiti obavještajnim službama da ih prevedu u konkretne smjernice, protokole, procedure i rokove koje je moguće primeniti unutar njihove organizacije.

Također, podesno je da osoblje nadzora bude svjesno negativnih posljedica koje njihovi zaključci mogu imati na pojedince iz obavještajne službe, s obzirom da često dovode do izricanja disciplinskih mjera, a ponekad i do otpuštanja. Iz tog razloga, obično se članovima nadzornih tijela savjetuje da o takvim pitanjima razgovaraju sa višim rukovodstvom prije nego što svoje zaključke unesu u svoj izvještaj.

11. IZVJEŠTAVANJE

Iako nadzorna tijela za obavještajne službe primjenjuju širok raspon procedura izvještavanja, pred njih se postavlja opća obaveza upoznavanja javnosti, državnih organa i službi sa rezultatima svojih istraga. U gotovo svim slučajevima, zakon od njih traži da podnose redovne izvještaje, obično na godišnjoj osnovi. Ti izvještaji obično sadrže opis poduzetih istraga i, u okviru mandata nadzornog tijela, budžetske analize. Izvještaji također mogu ponuditi preporuke, upućene obavještajnoj službi i/ili izvršnoj vlasti, u cilju unaprjeđenja odgovornosti, transparentnosti, zakonitosti i učinkovitosti službe.

Nadzorna tijela mogu, osim toga, podnositi specijalne izvještaje tokom cijele godine. Tu se može raditi o tematskim izvještajima ili opisima neke konkretne istrage. Na primjer, ukoliko nadzorno tijelo dođe do saznanja o nekoj spornoj aktivnosti obavještajne službe, obično ima obavezu pravovremeno izvijestiti o tome relevantni organ.

Prema Aidanu Willsu, „Nadzorna tijela obično rade dvije verzije svog izvještaja. Jedna verzija je namijenjena izvršnoj vlasti i obavještajnim službama i ona može sadržavati povjerljive informacije; druga verzija je namijenjena javnosti i ona obično ne sadrži povjerljive informacije. Nadzorna tijela obavljaju konsultacije sa predstavnicima izvršne vlasti i obavještajnim službama prije nego što objave svoj izvještaj za javnost. Na taj način se obavještajnim službama omogućuje da iskažu svoju eventualnu zabrinutost u pogledu unošenja osjetljivih informacija u izvještaj.[24]

11.1 PODNOŠENJE IZVJEŠTAJA

Načini podnošenja se razlikuju od zemlje do zemlje. U Belgiji, Odbor I dostavlja svoj godišnji izvještaj predsjedavajućim oba doma parlamenta, kao i nadležnom ministru. Međutim, specijalni izvještaji se prvo dostavljaju nadležnom ministru, a tek potom predsjedavajućem gornjeg doma parlamenta.[25] Dalje, izvještaj koji se podnosi parlamentu ne sadrži povjerljive informacije. U Kanadi, gdje se pravila koja se odnose na izvještavanje razlikuju, SIRC svoj godišnji izvještaj podnosi izvršnoj vlasti, koja ga potom mora proslijediti parlamentu u roku od petnaest dana. SIRC također ima zakonsku obavezu da obavi konsultacije sa CSIS-om prije nego što objavi izvještaj.

11.2 VLASNIŠTVO NAD IZVJEŠTAJIMA

Nadzorna tijela trebaju imati puno vlasništvo nad izvještajima, uključujući njihov sadržaj i vrijeme. U nekim slučajevima, zakoni ili pravilnici mogu diktirati poseban tretman povjerljivih informacija tokom nekog perioda prije nego što izvještaj postane javan. U Holandiji, CTIVD daje nadležnom ministru šest sedmica. Ako u tih šest sedmica nadležni ministar ne dostavi formalni odgovor, odnosni izvještaj nadzornog tijela za obavještajne službe se objavljuje.

11.3 POLITIČKI ASPEKTI

Obavještajne aktivnosti koje se odvijaju na marginama političkog legitimiteta mogu biti jako kontroverzne. Primjeri takvih aktivnosti su prikupljanje obavještajnih podataka na teritoriju druge zemlje, te korištenje posebnih istražnih radnji koje narušavaju ljudska prava osoba. Stoga nadzorne istrage često privlače pažnju stranaka koje žele iskoristiti nalaze nadzora za promoviranje vlastitih političkih interesa. Najbolji način da se nosi sa ovim pritiscima je biti spreman na njih. Na primjer, biti svjestan političkog kalendara i utjecaja koji on ima na pažnju novinara. Razmišljanje o političkim posljedicama koje će vjerojatno uslijediti nakon izvještaja može imati utjecaja na njegovu izradu. S duge strane, prevelika opreznost prilikom objavljivanja izvještaja može se odati dojam da je nadzorno tijelo suučesnik službe, umjesto da je neovisno i objektivno.

11.4 IMPLEMENTACIJA IZVJEŠTAJA

Izvještaj nije sam sebi cilj. Umjesto toga, njegova je svrha da pokrene diskusiju o pitanjima koja su predstavljena u izvještaju na parlamentu, vladi, i šire. Samo na taj način zaključci izvještaja mogu dovesti do implementacije njegovih preporuka.

Svaki izvještaj nadzora, bilo posebni bilo periodični, treba sadržavati listu zaključaka i preporučenih promjena. Njih treba precizno formulirati i numerirati. Osim toga, nakon što se izvještaj dostavi relevantnim organima, nadzorno tijelo treba s njima raditi na izradi

plana primjene. Potom, nadzorno tijelo treba izraditi i podnijeti novi izvještaj koji će navesti u kojoj mjeri je odnosna obavještajna služba primijenila preporuke.

11.5 DOSTUPNOST IZVJEŠTAJA

Korištenjem modernih tehnologija poput interneta, nadzorna tijela sada mogu svoje izvještaje učiniti dostupnima širokoj javnosti. Istraga u Ujedinjenom Kraljevstvu o uključenosti te zemlje u rat u Iraku (tzv. Chilcot istraga) je već objavila transkripte, izjave svjedoka i drugu nepovjerljivu dokumentaciju na svojoj internet stranici kao pripremu za objavljivanje svog konačnog izvještaja.

Može se desiti da se izvještaj nadzornog tijela stavlja na internet stranicu koja nije pod kontrolom samog nadzornog tijela – kao što je npr. stranica ministarstva ili parlamenta. Kako bi se postiglo da izvještaji budu dostupni javnosti, nadzorno tijelo treba insistirati na tome da unaprijed bude informirano o eventualnoj odluci da se izvještaji uklone sa internet stranice. Stoga se preporučuje da nadzorna tijela imaju stalne internet stanice dostupne najširoj javnosti koje će omogućiti lak pristup izvještajima i drugoj dokumentaciji.

12. POTENCIJALNI NALAZI

Nadzorna tijela za obavještajne službe razmatraju širok raspon pitanja, od kojih su neka opće prirode (kao što je zakonodavni okvir službe), a druga su specifičnija (kao što su istrage konkretnog događaja). U nastavku slijede primjeri tri potencijalna zaključka koji mogu proisteći iz istrage nadzornog tjela. U svakom se razmatraju preporuke za unaprjeđenje spornih oblasti.

12.1 OBAVJEŠTAJNA SLUŽBA NIJE PROVJERILA INFORMACIJE KOJE SU JOJ DOSTAVILI STRANI PARTNERI

Posebno kada djeluje u saradnji sa stranim partnerima, obavještajne službe možda neće svaki put na pravi način provjeriti informacije koje dobivaju iz vanjskih izvora. U Holandiji je 2009. godine, na primjer, CTIVD istraživao korištenje stranih obavještajnih podataka od strane Generalne obavještajno-sigurnosne službe (General Intelligence and Security Service - GISS), zaključivši da je GISS često propuštao da utvrdi, kako je predviđeno zakonom, da li je obavještajna agencija iz inostranstva ispunila sve kriterije za saradnju sa domaćom službom. Prema konačnom izvještaju CTIVD-a, „Nije utvrđeno postojanje strukturiranog procesa odlučivanja.“ Umjesto toga, izvještaj navodi: „Odluke su često donošene na ad hoc osnovi“, što je CTIVD kritizirao kao „previše ograničeno“ i „nepoželjno“: GISS-u je stoga upućen savjet da započne izradu dobro osmišljene procjene, ne samo kada stupa u nove odnose saradnje, nego i u pogledu već uspostavljenih odnosa.[26]

Provođenje ovakvih procjena prije poduzimanja radnji na osnovu dostavljenih obavještajnih podataka je od posebnog značaja kada su te dostavljene informacije dobivena mučenjem. Iz ovog razloga, Kanadska komisija za istragu djelovanja kanadskih zvaničnika u slučaju Maher Arar dala je preporuku da se svi sporazumi o vezama sa stranim službama rutinski podvrgnu ocjeni od strane nadzornih tijela.[27] Specijalni izvjestilac UN-a je isto tako preporučio da zemlje u svoje sporazume o razmjeni obavještajnih podataka uključe klauzulu koja uslovljava primjenu tog sporazuma ocjenom svojih nadležnih tijela i kojom se tim tijelima daje pravo da međusobno sarađuju u ocjenjivanju rada jedne ili obje

strane.[28] (Dalju raspravu na temu razmjene informacija pogledati u Poglavlju 7 - Roach).

12.2 OBAVJEŠTAJNA SLUŽBA JE PREKORAČILA SVOJ MANDAT

Nadzorna tijela moraju redovno obraćati pažnju da li su aktivnosti obavještajne službe prekoračile okvire njenog mandata, posebno kad se radi o korištenju posebnih ovlaštenja za tajno prikupljanje informacija (vidi Hutton – Poglavlje 5). Ukoliko se pokaže da je neka obavještajna služba stvarno propustila da ispoštuje zakonska ograničenja svojih ovlaštenja, nadzorno tijelo mora pozvati tu službu na odgovornost. To se može postići prijavljivanjem povrede nadležnim organima, i, ako je to u okviru mandata samog nadzornog tijela, prekidanjem korištenja jednog ili više specijalnih ovlaštenja službe za tajno prikupljanje informacija.

Komisija za slučaj Arar, nakon što je utvrdila, između ostalog, da je RCMP prekoračila svoj mandat, dala je preporuku da RCMP ubuduće poštuje posebnu ulogu CSIS-a u okviru kanadske obavještajne zajednice.[29]

12.3 OBAVJEŠTAJNA SLUŽBA JE ISPOLITIZIRANA

Obavještajni rad se može ispolitizirati na više načina, i ne odnose se svi na obavještajne službe koje dolaze do obavještajnih podataka. Najčešće, ipak, do politizacije dolazi zbog pretjerano bliskog odnosa između izvršne vlasti i zvaničnika službe koji svjesno ili nesvjesno prilagođavaju obavještajne podatke kako bi udovoljili nosiocima izvršne vlasti (eng. “intelligence to please”). Još jedan sličan oblik politizacije odnosi se na korištenje obavještajnih službi od strane zvaničnika vlade za dobivanje kompromitujućih informacija o svojim političkim protivnicima. Politizacija se također može pojaviti unutar obavještajne službe kada se njeni glavni analitičari natječu u izradi izvještaja po kojima će se poduzimati radnje, kako bi promovirali vlastitu karijeru.

Nadzorno tijelo koje dođe do dokaza o ispolitiziranosti obavještajne službe treba dati preporuku da parlament otvoreno razgovara o pravim zadacima spoljne i obrambene politike. Također, treba uzeti u obzir koje se zaštitne mjere mogu uvesti kako bi se spriječilo korištenje obavještajne službe kao političkog instrumenta u budućnosti.[30]

13. PREPORUKE

- Mandat nadzornog tijela za obavještajne službe se treba definirati na formalan, detaljan način, po mogućnosti u okviru sveobuhvatnog zakonskog okvira koji se odnosi na nadzor nad obavještajnim službama.
- Ukoliko dođe do promjene mandata obavještajne službe, i mandat nadzornog tijela za tu službu se treba izmijeniti u skladu s tim.
- Uzevši skupa, mandati nadzornih tijela za obavještajne službe jedne zemlje treba da pokriju cjelokupnu obavještajnu zajednicu te zemlje, uključujući civilnu i vojnu službu, kao i prateće odjele i zvaničnike.
- Prava pristupa, provođenja istrage i inspekcije koje nadzorno tijelo za obavještajne službe ima u okviru svog mandata treba da budu razmjerna ovlaštenjima obavještajne službe koju to tijelo nadzire.

- Nadzorno tijelo za obavještajne službe treba raspolagati ovlaštenjima da pregleda lokacije, održi zatvorena i otvorena saslušanja, te ostvari pristup povjerljivim informacijama u dokumentima, bazama podataka i drugim kompjuterskim arhivima.
- Nadzorno tijelo za obavještajne službe treba biti u mogućnosti vršiti *ex post* nadzor. U izuzetnim slučajevima, kada nadzorno tijelo za obavještajne službe vrši nadzor *ex ante*, njegovi članovi trebaju proći sigurnosnu provjeru od stane sigurnosne agencije kako bi se osiguralo da identiteti izvora i druge operativne informacije budu zaštićene.
- Da bi bolje organiziralo svoj rad i da bi potaklo veću posvećenost relevantnih aktera, nadzorno tijelo uvijek treba izraditi plan nadzora.
- Nadzorno tijelo za obavještajne službe treba održavati visoke profesionalne standarde. Na taj način se unaprjeđuje ne samo legitimitet nadzornog tijela, nego i, indirektno, legitimitet obavještajne službe koju nadzire.
- Rad nadzornog tijela za obavještajne službe treba biti transparentno, dosljedno i odgovorno.
- Nadzorno tijelo za obavještajne službe treba objavljivati periodične (godišnje) izvještaje u kojima opisuje svoje aktivnosti i nalaze. Također, treba po potrebi objaviti i posebne izvještaje u kojima se opisuju konkretne istrage.
- Izvještaji nadzornog tijela za obavještajne službe trebaju biti dostupni širokoj javnosti.
- Nadzorno tijelo za obavještajne službe treba dostavljati nacrt svojih zaključaka visokom rukovodstvu obavještajne službe kako bi mogli dati svoj odgovor u zakonskom roku.
- Izvještaji nadzornog tijela za obavještajnu službu uvijek treba da sadrže preporuke koje odnosna obavještajna služba može primijeniti.
- Nadzorno tijelo za obavještajnu službu treba da aktivno prati primjenu svojih preporuka i o tome objaviti odgovarajući izvještaj.

Bilješke

1. Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States," u *Democratic Control of Intelligence Services: Containing Rogue Elephants*, uredn. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), str. 12.
2. Committee on Foreign Affairs, 26.septembar 2003, 03-BuZa-61.
3. U interesu legitimiteta, obavještajne službe također trebaju djelovati u skladu sa javnim interesom. Konkretno, trebaju se uzdržati od zadiranja u privatnost pojedinaca na neutemeljen, nesrazmjeran i/ili nezakonit način.
4. Tommaso F. Giupponii Federico Fabbrini, "Intelligence agencies and the State secret privilege: the Italian experience," *International Constitutional Law Journal* Vol. 4, br. 3 (Fall 2010), str. 443–466 (dostupnona http://www.internationalconstitutionallaw.net/download/53c4319b67f44d52a392c655f17245a3/Giupponi_Fabbrini.pdf; verzija od 19. jula 2011.).
5. Posebne istražne radnje uključuju presretanje komunikacija, korištenje doušnika i prikrivenih isljednika, te formiranje maskirnihorganizacija.
6. Web stranica Kanadske sigurnosno-obavještajne službe (Canadian Security Intelligence Service web site), "Accountability and Review" (dostupno na: http://www.csis-scrs.gc.ca/bts/ccntblt-eng.asp; verzija od 17. avgusta 2011).
7. Općenito, preporuka je da se cjelokupna obavještajna zajednica jedne zemlje stavi pod nadzor barem jednog parlamentarnog odbora.
8. Web stranicapremijeraikabinetaAustralije (Australian Department of the Prime Minister and Cabinet), *Report of the Inquiry into Australian Intelligence Agencies*, Poglavlje 4 (dostupno na: http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter4/oversight.htm; verzija od 17. avgusta 2011).
9. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, br. 4 (decembar 2004), str. 6 (dostupnonahttp://www.pfpconsortium.org/file/1645/view; verzija od 19. jula 2011).
10. Guy Rapaille, "Le Comité permanent R dansu nrôled'organejuridictionnel: Le nouveau rôle du Comitébelgedans le cadre du contrôle des methods particulières de recueil de données" (govor održan na 6. Konferenciji parlamentarnih odbora za nadzor nad obavještajnim i sigurnosnim službama u zemljama članicama Evropske unije (6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States), Brisel, 30. septembra - 1. oktobra 2010.) (dostupno nahttp://www.parlement-eu2010.be/pdf/30sep-1okt-Thema0-Guy-Rapaille.pdf; verzija od 18. jula 2011).
11. Na primjer, pogledati United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011*, Cm 8114 (2011) (dostupno na http://www.cabinetoffice.gov.uk/sites/default/files/resources/isc-annualreport1011.pdf; verzija od 13. oktobra 2011).
12. Sandy Africa, "The South African Intelligence Services: A Historical Perspective," u *Changing Intelligence Dynamics in Africa*, uredn. S. Africa and J. Kwadjo (Birmingham, UK: Global Facilitation Network for Security Sector Reform/African Security Network, 2009), str. 61–94.
13. Raspravu na ovu temu vidjeti Paul Robinson, *Eyes on the Spies: Reforming Intelligence Oversight in Canada*, Centre for International Policy Studies (CIPS) Policy Brief No. 1 (Ottawa: CIPS, University of Ottawa, November 2008) (dostupno na http://www.sciencessociales.uottawa.ca/cepi-cips/eng/documents/CIPS_PolicyBrief_Robinson_Nov2008.pdf; verzija od 17. avgusta 2011).
14. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), str. 351 (dostupno na: http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; verzija od 17. avgusta 2011).
15. Web stranica Iraq Inquiry, "About the Inquiry" (dostupno na http://www.iraqinquiry.org.uk/about.aspx; verzija od 18. avgusta 2011).
16. Raspravu o norveškom sistemu nadzora nad obavještajnim službama gdje je usvojen ovaj pristup vidjeti u TrygveHarvold, "Norwegian Parliamentary Oversight: an 'effective remedy'?" (govor na 6. konferenciji parlamentarnih odbora za nadzor nad obavještajnim i sigurnosnim službama zemalja članica Evropske unije (6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States), Brisel, 30. Septembar - 1. oktobar 2010) (dostupno na http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema1-Trygve%20Harvold.pdf; verzija od 18. jula 2011).
17. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (decembar 2004), str. 9 (dostupno na http://www.pfpconsortium.org/file/1645/view; verzija od 19. jula 2011).
18. The UN Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including*

the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations Document A/HRC/10/3 (4. februar 2009), str. 24 (dostupno na http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; verzija od 18. avgusta 2011).

19. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, br. 4 (decembar 2004), str. 3 (dostupno na http://www.pfpconsortium.org/file/1645/view; verzija od 19. jula 2011).
20. Web stranica Australian Department of the Prime Minister and Cabinet, *Report of the Inquiry into Australian Intelligence Agencies*, Poglavlje 8, Preporuka 22 (dostupno na http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter8/1_findings.htm; verzija od 17. avgusta 2011).
21. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), Poglavlje 9 (dostupno na http://www.sirc-csars.gc.ca/pdfs/cm_arar_rec-eng.pdf; verzija od 19. oktobra 2011).
22. Za raspravu o ovoj istrazi pogledati Parlement&Politiek web site, "Parlementaireenquêteopsporingsmethoden, IRT (1994-1996)" (dostupnonahttp://www.parlement.com/9291000/modulesf/g8pdkcx4; verzija od 19. jula 2011).
23. Ovaj sažetak je izveden iz primjera plana prezentiranog u United States Army Inspector General School, *Intelligence Oversight Guide* (februar 2008), Appendix D (dostupno na http://www.fas.org/irp/doddir/army/ioguide.pdf; verzija od 15. jula 2011).
24. Aidan Wills, *Guidebook: Understanding Intelligence Oversight*, Toolkit—Legislating for the Security Sector (Geneva: DCAF, 2010), str. 40.
25. Ibid., str. 37.
26. Bert van Delden, "Partners in Business?" (govorodržanna 6. konferencijiparlamentarnihodborazanadzornadobavještajnimisigurnosnimslužbamazemaljačlanicaEvropskeunije, Brisel, 30. septembar- 1. oktobar 2010), str. 4 (dostupno na http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema3-Bert%20Van%20Delden.pdf; verzija od 18. jula 2011).
27. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006) (dostupno na http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; verzija od 17. avgusta 2011).
28. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4. februar 2009), str. 21 (dostupno na http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; verzija od 18. avgusta 2011). Referencana C. Forcese, T*he Collateral Casualties of Collaboration: the Consequence for Civil and Human Rights of Transnational Intelligence Sharing* (prezentacijaza DCAF radionicu o odgovornosti međunarodne obavještajne saradnje, Oslo, 17. oktobar 2008).
29. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), str. 312 (dostupnonahttp://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; verzija od 17. avgusta 2011).
30. Za daljnju diskusiju, vidjeti u Monica den Boer, "Keeping 'Spies & Spooks' on the Right Track: Ethics in the Post 9/11 Intelligence Era," u *Ethics and Security*, uredn. Monica den Boer i Emile Kolthoff (The Hague: Eleven, 2010), str. 57–83.

POGLAVLJE 5

Nadzor nad prikupljanjem informacija

Lauren Hutton

PET

5

Nadzor nad prikupljanjem informacija

Lauren Hutton

1. UVOD

Svrha ovog poglavlja je razmotriti ulogu nadzornih tijela u praćenju funkcija prikupljanja informacija obavještajnih službi. Proizvodnja obavještajnih informacija je proces koji se sastoji od više koraka i zahtijeva raspodjelu zadataka, planiranje, prikupljanje informacija, njihovu analizu i diseminaciju. Ipak, od svih ovih koraka, prikupljanje informacija, posebno korištenjem tajnih sredstava, ostaje karakteristika koja određuje obavještajne službe, barem u očima javnosti. Prikupljanje informacija je jedan od najkontroverznijih aspekata obavještajnog rada i predstavlja neobičan zbir izazova za nadzorna tijela zadužena za očuvanje demokratskih ideala.

Prvi dio poglavlja razmatra neke od metoda kojim obavještajne službe prikupljaju informacije. Potom će razmotriti načine na koje demokratske zemlje mogu primjenjivati zakone, davati saglasnosti i vršiti nadzor primjene mjera tajnog prikupljanja podataka kako bi osigurale da se tom prilikom ljudska prava poštuju.

2. IZVORI I METODE PRIKUPLJANJA PODATAKA

Osnova obavještajnog rada su informacije prikupljene iz raznih izvora. Ukoliko ne postoji jedan izvor koji može pružiti dovoljno informacija za potpuno razumijevanje određenog

pitanja, obavještajne službe koriste višestruke izvore kako bi došle do najtačnije slike događaja. Ovi izvori se obično kategoriziraju prema tipu:

- informacije dobijene iz ljudskih izvora (eng. HUMINT), npr. doušnici;
- informacije dobijene presretanjem komunikacija (eng. SIGINT);
- informacije dobijene iz otvorenih, javnih izvora (eng. OSINT), npr. medijski izvještaji;
- informacije dobijene vazdušnim i kosmičkim izviđanjem i snimanjem (eng. IMINT), npr. satelitske fotografije.

Metode prikupljanja informacija mogu biti otvorene ili tajne. Otvorene metode se najčešće koriste kako bi se prikupile informacije tipa OSINT, jer se te informacije otvoreno čuvaju i dostupne su javnosti. Zatvorene, ili tajne metode prikupljanja informacija, koriste tajnost kako bi se prikupile informacije o objektima od interesa, a da oni pri tom toga nisu svjesni. Tajne metode mogu uključiti korištenje doušnika, presretanje informacija, elektronsko i fizičko praćenje, te fotografiranje. Kada se te metode koriste na način koji privremeno ograničava pravo pojedinca na privatnost, zovemo ih „intruzivnim metodama istrage“, a same te tehnike se nazivaju „posebne istražne mjere“ ili „posebne istražne tehnike“.

Vijeće Evrope je definiralo posebne *istražne tehnike* kao „tehnike primijenjene od nadležnih vlasti u svrhu otkrivanja i vođenja krivičnih istraga ozbiljnih krivičnih djela, sa ciljem prikupljanja informacija bez znanja osumnjičenih.“[1] U ovom kontekstu, pojam *nadležne vlasti* može značiti obavještajne službe ili agencije za provedbu zakona. Važno je ovdje zapaziti da u mnogim zemljama obavještajne službe koriste takve mjere ne samo u kontekstu krivičnih istraga, već i u sklopu preventivnih istraga vezanih za nacionalnu sigurnost. Opći je princip da se metod koji se koristi za prikupljanje informacija treba zasnivati na tipu potrebnih informacija, svrsi prikupljanja informacija, te na operativnom, zakonskom i političkom kontekstu u kojem obavještajne službe rade.

3. UTJECAJ PRIKUPLJANJA INFORMACIJA NA LJUDSKA PRAVA

Obavještajne službe prikupljaju informacije kako bi pomogle izvršnoj vlasti u definiranju politika i donošenju strateških i operativnih odluka. Način na koji one prikupljaju informacije treba da bude u skladu sa prioritetima i vrijednostima društva kojem služe.[2] U demokratskim zemljama, obavještajne službe treba da poštuju ljudska prava, vladavinu prava i principe demokratskog upravljanja, uključujući odgovornost, transparentnost i participatorno odlučivanje. Obavještajni proces od dodjele zadataka do diseminacije treba da funkcionira unutar ovih parametara.

Prikupljanje informacija o sigurnosnim prijetnjama može direktno utjecati na temeljna prava pojedinaca.[3] Prema izvještaju Južnoafričke ministarske komisije za ocjenu rada obavještajnih službi za 2008. godinu, koja istražuje slučajeve u kojima postoji sumnja u pogledu zloupotrebe ovlasti od strane Nacionalne obavještajne agencije, „intruzivne metode istrage mogu igrati ključnu ulogu u otkrivanju kriminalnih aktivnosti i urota, ali mogu biti i zloupotrijebljene sa ciljem podrivanja demokratskog procesa, miješanja u zakonitu političku i društvenu aktivnost, te osiguravanja nepravedne prednosti za neke političare i partije.”[4]

Dok je korištenje intruzivnih metoda od strane države uvijek ustavno i politički osjetljivo, njihovo korištenje od strane obavještajnih službi mora se tretirati sa posebnim oprezom. Razlozi za ovaj oprez, navedeni u izvještaju spomenute Ministarske komisije,[5] uključuju sljedeće:

- osoba pod istragom možda nikad neće saznati da su nad njom korištene intruzivne metode, te stoga neće moći uložiti prigovor niti osporiti njihovu validnost na sudu;
- visok nivo tajnosti koji okružuje intruzivne metode smanjuje sposobnost nadzornih tijela da prate njihovo korištenje, te da otkriju moguće zloupotrebe i nezakonitosti;
- mjera u kojoj intruzivne metode krše pravo pojedinca na privatnost može biti mnogo veće nego što je potrebno ili namjeravano;
- pored kršenja privatnosti praćenih lica, intruzivne metode često krše prava na privatnost pojedinaca sa kojima je ta osoba u kontaktu, čak i kad ti pojedinci nisu predmet istrage;
- osjetljive informacije o osobi pod istragom i informacije o ljudima sa kojima je ta osoba u kontaktu bilježe se i čuvaju u obavještajnoj službi čak i nakon trajanja same istrage, te se ponekad koriste u druge svrhe.

Nekada se razlikuje vanjska i unutrašnja primjena tehnologije presretanja komunikacija, zato što unutar zemlje postoji opasnost da izvršna vlast koristi tajne metode presretanja komunikacija u partijske svrhe, kao što je špijuniranje političkih protivnika. Presretanje stranih komunikacije, s druge strane, općenito ne ugrožava domaći demokratski poredak.

U demokratskim zemljama, tijela za nadzor nad obavještajnim službama imaju legitimno pravo, a često i zakonsku odgovornost, da osiguraju da se obavještajne službe ponašaju na način koji je u skladu sa ustavnim poretkom. Nadzorna tijela obično imaju takav opseg odgovornosti koji obuhvata cijeli obavještajni ciklus, ali područje prikupljanja informacija zahtijeva posebnu pažnju zbog prijetnje koju tajne, intruzivne metode predstavljaju za demokratske vrijednosti. Nadzorna tijela trebaju posebno pažljivo pratiti korištenje svih takvih metoda, kako bi osigurala da ponašanje obavještajnih službi ostane u okviru zakona.

3.1 ZAŠTITA PRAVA NA PRIVATNOST

Pravo koje obavještajne službe najčešće ograničavaju ili krše je pravo na privatnost. Stoga ključna funkcija nadzornih tijela nad obavještajnim službama treba da bude osiguravanje da službe prikupljaju informacije na način koji je u skladu sa domaćim i međunarodnim zakonima o pravu na privatnost.

Specijalni izvjestilac UN-a za promociju i zaštitu ljudskih prava i temeljnih sloboda prilikom borbe protiv terorizma definirao je pravo na privatnost kao „pretpostavku da pojedinci treba da imaju određeno područje autonomnog razvoja, interakcije i slobode, 'privatnu sferu' sa ili bez interakcije sa drugima koje je slobodno od intervencije države i slobodno od pretjerane, neovlaštene intervencije drugih nepozvanih pojedinaca."[6]

Slično, Član 17. Međunarodnog pakta o građanskim i političkim pravima navodi da:

1. *Niko ne može biti izložen proizvoljnom ili nezakonitom miješanju u privatni život, porodicu, stan ili prepisku, niti protivzakonitim napadima na čast i ugled.*
2. *Svako ima pravo na zakonsku zaštitu od takvog miješanja ili napada.*

Sa svojih 167 potpisnica,Međunarodni pakt o građanskim i političkim pravima čini osnovu za međunarodni zakon o pravu na privatnost. Pošto se privatnost smatra temeljnim ljudskim pravom, akcije koje preduzimaju vlade kojima se ograničava to pravo moraju biti zasnovane na domaćem zakonu i moraju se obavljati u specifične, legitimne svrhe.

Kako je utvrdio Evropski sud za ljudska prava, zaštita nacionalne sigurnosti je legitimna svrha za ograničavanje ljudskog prava, kao što je pravo na privatnost. Međutim, prema ocjeni ovog Suda, svako takvo ograničavanje mora biti nametnuto u skladu sa nacionalnim zakonima, što mora uključiti garancije protiv zloupotrebe i pravne lijekove, ukoliko se zloupotrebe ipak dogode.[7]

Korištenje tajnih, intruzivnih metoda prikupljanja informacija od strane obavještajne službe predstavlja ograničenje prava na privatnost. Stoga, svako takvo korištenje mora biti zasnovano na domaćem zakonu i provoditi se samo u specifične, legitimne svrhe. U Južnoj Africi, bivši generalni inspektor za obavještajne službe tumačio ga je na sljedeći način:

> *Ograničenje prava mora biti opravdano na osnovu prijetnje za nacionalnu sigurnost. Takvo ograničenje treba da prođe test srazmjernosti, koji uključuje prirodu prava i značaj razloga ograničenja tog prava. Stoga, kapacitet za prikupljanje informacija treba da bude usklađen sa jednako čvrstim garancijama koje štite ustavna prava građana i održavaju otvoreno i demokratsko društvo.*[8]

3.2 UTJECAJ TEHNOLOGIJE NA PRIKUPLJANJE INFORMACIJA

Moderna informacijska i komunikacijska tehnologija omogućava pojedincima diljem svijeta da neposredno međusobno komuniciraju, te da informacije smjesta stignu do najudaljenijih mjesta. Međutim, to također omogućava vladama da provode dosad neviđeni nivo nadzora. Korištenjem naprednih tehnoloških sredstava, obavještajne službe mogu prikupljati informacije u ogromnoj količini, pri čemu one prikupljaju mnogo više informacija nego što uopće mogu apsorbirati i analizirati. Pošto je to prikupljanje informacija po svojoj prirodi nasumično, ono u sebi krije mogućnost kršenja ljudskih prava, te se treba preduzimati samo u okviru zakona koji štiti pravo na privatnost.

Sistem presretanja komunikacija ECHELON nudi ovdje koristan primjer. Ovaj sistem - kojim rukovode zajednički Sjedinjene Države, Ujedinjeno Kraljevstvo, Australija, Kanada i Novi Zeland kao dio kolektivnog sigurnosnog aranžmana - presreće signale koji prolaze do i od satelita u Zemljinoj orbiti. Evropski parlament je 2000. godine osnovao Privremeni odbor za istragu o potencijalnom utjecaju sistema ECHELON na prava pojedinaca na osnovu Zakona Evropske unije (EU). Završni izvještaj ovog Odbora u svom zaključku navodi kako masovni sistemi presretanja informacija, kakav je ECHELON, imaju potencijal kršenja prava na privatnost zato što ne poštuju princip srazmjernosti u pogledu korištenja intruzivnih metoda. Mada priznaje da takvi sistemi presretanja komunikacija mogu biti opravdani na osnovu nacionalne sigurnosti, Odbor preporučuje da se prilikom njihovog korištenja treba rukovoditi jasnim i dostupnim zakonima, te da države članice EU trebaju uspostaviti rigorozne mjere nadzora.[9]

4. PRAVNI OKVIRI ZA PRIKUPLJANJE INFORMACIJA

U većini demokratskih zemalja, prikupljanje informacija od strane obavještajnih službi definirano je zakonskim okvirom koji osigurava odgovornost i transparentnost. To se

obično čini tako što su odgovornosti za davanje saglasnosti i nadzor izuzeti iz isključive nadležnosti izvršne vlasti, te se dijele (u različitim stepenima) između parlamenta, sudstva i tijela koja ne pripadaju izvršnoj vlasti.

Međunarodni zakoni mogu pomoći u izradi državnih zakona. Na primjer, 2005. godine, Vijeće Evrope je izdalo sljedeće preporuke za izradu domaćih zakona o korištenju posebnih istražnih tehnika u krivičnim istragama:[10]

1. *Države članice treba da, u skladu sa zahtjevima Evropske konvencije o ljudskim pravima (ETS br. 5), definiraju u svojim domaćim zakonima slučajeve u kojima, te uslove pod kojima, nadležni organi imaju ovlast da koriste posebne istražne tehnike.*
2. *Države članice treba da preduzmu odgovarajuće zakonodavne mjere koje će omogućiti, u skladu sa stavom 1, korištenje posebnih istražnih tehnika od strane nadležnih organa u mjeri u kojoj je to potrebno u demokratskom društvu i samo onda kada se smatra odgovarajućim radi djelotvorne krivične istrage i krivičnog gonjenja.*
3. *Države članice treba zakonima da osiguraju da sudske vlasti ili druga nezavisna tijela vrše adekvatnu kontrolu provedbe posebnih istražnih tehnika, kroz prethodno davanje saglasnosti njihove provedbe, nadzor nad njima tokom istrage, ili naknadnu (ex post facto) ocjenu primijenjenih mjera.*

Općenito, domaći zakoni koji se tiču korištenja tajnih, intruzivnih metoda prikupljanja informacija treba da specificiraju:

- kada se takve metode mogu koristiti;
- koje indicije treba da su prisutne da bi se metode mogle primijeniti („osnovi sumnje“);
- koja se ograničenja primjenjuju;
- koje saglasnosti su potrebne primjenu metoda.

Primjeri specifičnih domaćih zakona koji se odnose na korištenje tajnih, intruzivnih metoda prikupljanja informacija unutar zemlje uključuju australijski Zakon o presretanju i pristupu telekomunikacijama, australijski Zakon o komunikacijskoj pomoći u provedbi zakona, američki Zakon o praćenju stranih obavještajnih službi, te Zakon o reguliranju istražnih ovlasti Ujedinjenog Kraljevstva. Svaki takav zakon treba da riješi sljedeća tri ključna pitanja:

- dopustive ciljeve;
- srazmjernost;
- saglasnost i nadzor.

Općenito govoreći, oni treba da zahtijevaju od nadležnih vlasti da budu razložno sigurni da će tajne, intruzivne metode kao rezultat polučiti informacije za kojim tragaju.

4.1 DOPUSTIVI CILJEVI

Dopustivi ciljevi za korištenje tajnih, intruzivnih metoda prikupljanja informacija razlikuju se znatno od države do države. U nekim zemljama, kako je to preporučilo Vijeće Evrope, vođenje krivične istrage je dopustivi cilj.[11] U drugim, zaštita nacionalne sigurnosti i odbrana demokratskog poretka su također dopustivi ciljevi. Član 3(1) Njemačkog zakona kojim se ograničava privatnost prepiske, pošte i telekomunikacija daje ovlasti Njemačkoj vladi (tj., sigurnosnim službama uključujući policiju i obavještajne službe) da izdaju naredbu o

ograničenjima prava na privatnost nekog pojedinca ako „konkretne indicije daju osnova za sumnju da ta osoba planira, čini ili je počinila" krivično djelo protiv:

- mira;
- demokratskog poretka;
- nacionalne sigurnosti;
- sigurnosnih trupa stacioniranih u Njemačkoj.

Termin *konkretne indicije* utvrđuje visoki prag koji se mora ispuniti prije nego što se tajne, intruzivne metode mogu primijeniti. Kako bi se osiguralo da postoje značajni razlozi za korištenje intruzivnih metoda istrage, takvo obrazloženje treba da bude uključeno u zahtjev za saglasnost primjene ovih metoda.

4.2 SRAZMJERNOST

Zakoni o korištenju tajnih, intruzivnih metoda prikupljanja informacija treba da zahtijevaju da stepen intruzivosti bude srazmjeran cilju istrage. U tom pogledu, Vijeće Evrope je preporučilo da se posebne istražne tehnike koriste samo kada:

- postoje uvjerljivi osnovi sumnje da je ozbiljno krivično djelo počinjeno, ili da se planira;
- treba posvetiti dužnu pažnju „srazmjernosti između učinka korištenja posebnih istražnih tehnika i cilja koji je identificiran."[12]

Vijeće Evrope je dalje preporučilo da države članice koriste manje intruzivne metode kada god „takve metode omogućavaju da se adekvatno i učinkovito otkrivaju, sprječavaju ili krivično gone takva krivična djela."[13] Smjernice poput ovih omogućavaju korištenje intruzivnih metoda u legitimne svrhe, dok se na najmanju moguću mjeru svodi zloupotreba ili kršenje ljudskih prava.

Princip srazmjernosti je teže primijeniti u vezi sa prijetnjama po nacionalnu sigurnost. U ovom slučaju, osnovni kriterijum treba da bude to da se informacija ne može prikupiti manje intruzivnom metodom, već da je jedino intruzivnom metodom moguće doći do tražene informacije. Na primjer, u Njemačkoj, naredbe za korištenje metoda prikupljanja koje ograničavaju pravo na privatnost mogu se izdati samo „tamo gdje bi korištenje drugog metoda istrage činjenica bilo uzaludno ili bi, pak, znatno otežalo istragu."[14]

4.3 DAVANJE SAGLASNOSTI I NADZOR

Kako bi se spriječila zloupotreba tajnih, intruzivnih metoda prikupljanja informacija, zakonom treba definirati davanje saglasnosti (u kojima učestvuju viši rukovodioci obavještajne službe i sudstvo) i mehanizme nadzora (u kojima učestvuju parlament i stručna nadzorna tijela). Odgovarajuće strukture za davanje saglasnosti i nadzora će biti predmet detaljne rasprave u sljedeća dva dijela ovog dokumenta. Ti nivoi ovlaštenja i nadzora ne isključuju se uzajamno, a jedan sveobuhvatan i razvijen sistem odgovornosti i transparentnosti može uključiti davanje saglasnosti sa više od jednog nivoa i više od jednog mehanizma nadzora.

5. DAVANJE SAGLASNOSTI ZA OPERACIJE PRIKUPLJANJA INFORMACIJA

Različiti tipovi operacija prikupljanja informacija zahtijevaju različite nivoe saglasnosti. Na primjer, fizičko praćenje, mada tajno, nije veoma intruzivno, te je obično dovoljna interna saglasnost obavještajne službe. Prisluškivanje telefona, međutim, ili presretanje pošte predstavlja veće kršenje privatnosti te stoga zahtijeva davanje saglasnosti sa višeg nivoa, kao što je ministar odgovoran za obavještajnu službi i/ili sudija. Svako obnavljanje operacija tajnog prikupljanja podataka treba da uključi isti nivo davanja saglasnosti kao i originalni zahtjev.

5.1 INTERNA SAGLASNOST

Zahtjev da više rukovodstvo obavještajne službe daje saglasnost za korištenje posebnih istražnih tehnika potpadaju pod odgovornost same službe i time na značajan način odvraća službenike od prekršaja. Mada ovaj zahtjev možda nije dovoljan sam po sebi kako bi se spriječila zloupotreba, on ukazuje na to da je odluka da se ograniči pravo na privatnost jednog pojedinca ozbiljna, teška odluka i ne smije se olako uzimati. Unutar službe, organ koji donosi odluke treba da bude strukturiran tako da što je veće zadiranje u privatnost, to se zahtijeva veći nivo za davanje saglasnosti.

5.2 SAGLASNOST IZVRŠNE VLASTI

Obavještajne službe kontrolira izvršna vlast, koja postavlja njihove prioritete i usmjerava njihove aktivnosti. To je obično odgovornost određenog ministra. Isti taj ministar može također biti odgovoran za davanje saglasnosti za specifične operacije prikupljanja informacija. Kao što interni zahtjev za davanje saglasnosti osigurava da više rukovodstvo službe snosi odgovornost za korištenje posebnih istražnih tehnika od strane obavještajne službe, isto se to odnosi i na procedure davanja saglasnosti od strane izvršne vlasti u pogledu odluke nadležnog ministra da odobri određene mjere.

Zloupotreba na ministarskom nivou najčešće uključuje korištenje mehanizama za prikupljanje informacija od strane obavještajne službe kako bi se prikupile povjerljive informacije o političkim protivnicima vlasti. Iz tog razloga, u pogledu korištenja tajnih metoda prikupljanja informacija u okviru matične države, pravni okvir treba da uključi procedure davanja saglasnosti koje:

- utvrđuju ograničenja u pogledu toga šta ministar može tražiti od službe da uradi;
- pored ministarske, zahtijevaju i sudsku saglasnost za korištenje intruzivnih metoda prikupljanja informacija;
- stvaraju mehanizme kojim obavještajni službenici mogu prijaviti prekršaje;
- utvrđuju nezavisno nadzorno tijelo za ocjenu vođenja takvih operacija.

5.3 SUDSKA SAGLASNOST

U većini demokratskih zemalja, tradicionalna odgovornost sudstva je zaštita ljudskih prava pojedinaca. S obzirom na tu ulogu, logično je da sudije dobiju zadatak ocjene zaštite ljudskih prava u odnosu na potrebe za prikupljanjem informacija obavještajnih službi. Uobičajena je praksa, stoga, da domaće zakonodavstvo zahtijeva od obavještajnih službi da dobiju sudsku saglasnost (obično u obliku sudskog naloga) prije nego što prekrše

pravo na privatnost nekog pojedinca. Takvi nalozi, zato što su proizvod nepristrasne procjene, smatraju se važnom kontrolom moguće zloupotrebe.[15] Nadalje, kao što je zapazila Venecijanska komisija u svom izvještaju o demokratskom nadzoru sigurnosnih službi, zahtjev u pogledu sudske saglasnosti podređuje pitanja sigurnosti zakona te time institucionalizira poštivanje zakona.[16]

Dobra je praksa da zakoni konkretno navedu tip operacija koje zahtijevaju sudsku saglasnost, kao i to koliko veliko ovlaštenje može imati sudija u pogledu ograničavanja opsega, trajanja i predmeta operacije. Zakon treba također da propiše da svaki zahtjev za izdavanje naloga za primjenu mjera mora sadržavati određeni minimum informacija kako bi bio validan (vidjeti Okvir 1).

Okvir 1: Zahtjevi u pogledu podnošenja zahtjeva za sudsku saglasnost u Kanadi

Kanadski zakon o sigurnosno-obavještajnoj službi zahtijeva da obavještajna služba u svom zahtjevu za sudskim nalogom za presretanje komunikacija uključi sljedeće informacije:[17]

- činjenice na osnovu kojih opravdava uvjerenje da postoji prijetnja za nacionalnu sigurnost;
- dokazi da su manje intruzivne tehnike pokušane i nisu uspjele, ili razlozi zašto one vjerovatno neće uspjeti;
- tip komunikacija koje će se presretati;
- tip informacija koje će se prikupiti;
- identitet osoba ili grupe osoba koje su predmet istrage;
- identitet osoba, ako je poznat, čije komunikacije će biti presretane;
- opći opis mjesta, ako je poznato, gdje će nalog biti izvršen;
- period za koji se zahtijeva nalog;
- detalji bilo kojeg prethodnog zahtjeva koji je podnesen u vezi sa osobom identificiranoj u aktualnom zahtjevu – uključujući datum prethodnog zahtjeva, ime sudije kome je prethodni zahtjev podnesen, te odluka sudije o tom zahtjevu.

U mnogim zemljama, sudski nalog je potreban za presretanje komunikacija. Argentinski Zakon o nacionalnoj obavještajnoj službi, na primjer, zahtijeva da obavještajne službe u zemlji dobiju sudsku saglasnost prije presretanja privatnih komunikacija bilo kojeg tipa.[18]

Zakon ponekad nalaže da zahtjevi obavještajne službe budu predmet odluke specijaliziranih sudija. Kanada, Francuska, Južna Afrika i Španija, između ostalih država, slijede tu praksu. Neke zemlje osnovale su čak specijalne sudove za davanje sudske saglasnosti za primjenu posebnih mjera. Među njima je američki Sud za nadzor nad vanjskim obavještajnim službama (FISC), koji je osnovan prema Zakonu o stranim obavještajnim službama iz 1978. godine. Ovaj sud, kojeg čine jedanaest sudija saveznih okružnih sudova koji se ne biraju svi istovremeno, već se svake dvije godine bira jedna trećina novih članova na jedan mandat u trajanju od maksimalno sedam godina, ocjenjuje zahtjeve za izdavanje naloga u pitanjima nacionalne sigurnosti. Navedenim Zakonom je također uspostavljen Revizorski sud za nadzor nad vanjskim obavještajnim službama, koji odlučuje o žalbama vlade na odluke FISC-a.[19]

Ponekad ove specijalizirane sudije i sudovi imaju ovlast da ocjenjuju operacije prikupljanja informacija još dok su u toku. U Južnoj Africi, Zakon o reguliranju presretanja komunikacija i pružanje informacija vezanih za komunikacije iz 2002. godine omogućava sudijama da zahtijevaju privremene pisane izvještaje o napretku postignutom u pogledu postizanja ciljeva navedenih u nalogu.[20] Na taj način, oni mogu spriječiti ugrožavanje privatnosti osoba koje nisu predviđene nalogom, te osigurati da se tajne, intruzivne metode ne primjenjuju duže nego što je potrebno.

6. NADZOR NAD OPERACIJAMA PRIKUPLJANJA INFORMACIJA

Pored davanja saglasnosti za početak operacija tajnog prikupljanja podataka, od velike je važnosti i to da one budu pod nadzorom tokom njihove primene kako bi se ocijenilo da li obavještajne službe poštuju izdato odobrenje u praksi. Samo kada obje ove garancije, davanje saglasnosti i nadzor, postoje, može se smatrati da su operacije prikupljanja informacija regulirane ne valjan i djelotvoran način (za diskusiju o rješavanju žalbi protiv obavještajnih službi od strane nadzornih tijela, vidjeti Poglavlje 9 – Forcese).

Nadzor mogu obavljati brojna tijela. Neka, kao glavna revizorska institucija i nacionalna institucija ombudsmena, relevantne su zbog svog širokog mandata. Ostale, kao što su generalni inspektori i stručna nadzorna tijela, imaju specijalizirano stručno znanje koje podržava njihov specifični mandat. Većina zemalja dijeli nadzor između nekoliko tijela čije nadležnosti se preklapaju u različitom stepenu.

6.1 PARLAMENTARNA NADZORNA TIJELA

U demokratskim porecima, parlamenti su odgovorni za uspostavu pravnih okvira u kojima djeluju vladina tijela. Ona također imaju odgovornost da prate poštivanje zakona koje usvajaju. Te odgovornosti se primjenjuju na obavještajne službe baš kao i na sve druge vladine agencije.

Međutim, pošto se obavještajne službe razlikuju po mnogo čemu od drugih vladinih agencija, parlamenti obično osnivaju odbore za nadzor nad obavještajnim službama kako bi pratili aktivnost službe i preporučivali revizije pravnog okvira u kojem one djeluju. U pogledu operacija prikupljanja informacija, ti odbori obično imaju ovlaštenje za:

- nadziranje korištenja tajnih, intruzivnih metoda;
- praćenje izrade budžeta i korištenje sredstava;
- kontrolu nad pravnim okvirom kako bi se osiguralo da sadrži dovoljne garancije za zaštitu ljudskih prava;
- osiguranje da obavještajne službe poštuju pravni okvir.

Usto, zakon koji regulira ovu oblast može ovlastiti parlamentarne odbore da nadziru tajne, intruzivne operacije prikupljanja informacija. Parlamentarni nadzorni odbori mogu igrati bitnu ulogu u osiguravanju da se procedure davanja saglasnosti ispravno primjenjuju. Na primjer, Zakon o nacionalnoj obavještajnoj službi Argentine ovlašćuje Zajednički odbor za nadzor nad obavještajnim agencijama i njihovim aktivnostima da nametnu izradu (i podnošenje odboru) izvještaja u kojem se navodi spisak „presretanih komunikacija i njihovih snimaka koji su obavljeni u datom periodu."[21] Odbor onda može koristiti taj spisak

da provjeri korištenje posebnih istražnih tehnika u odnosu na date saglasnosti nadležnih organa. Na taj način, ovaj odbor može potvrditi da li su procedure davanja saglasnosti na propisan način provedene (vidjeti Okvir 2 dolje radi primjera).

Okvir 2: Parlamentarni nadzor nad prikupljanjem informacija u Njemačkoj

U Njemačkoj, korištenje intruzivnih metoda prikupljanja informacija nadzire Parlamentarni kontrolni panel.

Zakon zahtijeva da izvršna vlast dostavi kontrolnom panelu izvještaj o korištenju intruzivnih metoda „u intervalima ne dužim od 6 mjeseci". Na osnovu tih periodičnih izvještaja, panel priprema godišnji izvještaj za Bundestag o prirodi i opsegu intruzivnih metoda koje se primjenjuju prema ovom zakonu.[22]

Uz ovu funkciju praćenja, zakon također kontrolnom panelu daje ulogu tijela koje daje saglasnost. Savezna obavještajna služba (vanjska obavještajna služba) mora dobiti saglasnost kontrolnog panela prije nego što presretne međunarodni komunikacijski saobraćaj koji se prenosi „u obliku paketa", a može imati veze sa Njemačkom ili njemačkim državljanima. To su presretanja komunikacija koja se zapravo zasnivaju na ključnim riječima, koje ne ciljaju na specifične komunikacije.[23]

Članstvo u parlamentarnom nadzornom odboru ne zahtijeva generalno bilo kakvo stručno znanje u pogledu obavještajnog rada. Međutim, kao što je zapazio jedan član američkog Kongresa, da bi se donijele odgovarajuće odluke, članovi odbora moraju se upoznati sa prirodom obavještajnih informacija, kao i sa metodama korištenim za njihovo prikupljanje, obradu i stvaranje.[24]

6.2 STRUČNA NADZORNA TIJELA

Stručna tijela za nadzor nad obavještajnim službama su nezavisna tijela čiji članovi i uposlenici imaju posebno stručno znanje u pogledu obavještajnog rada (vidjeti Born i Geisler – Poglavlje 1). Jedan od najčešćih tipova stručnih nadzornih tijela je generalni inspektor. Mada njegova funkcija i odgovornost varira od države do države, generalni inspektor obično je nezavisno tijelo ovlašteno da prima i djeluje po žalbama u pogledu zakonitosti ponašanja obavještajne službe. Njegov mandat obično uključuje pravo da provodi istrage o korištenju posebnih istražnih tehnika i tajnih metoda prikupljanja informacija. U nekim zemljama, kao što su Sjedinjene Države i Kanada, on djeluje unutar obavještajne službe. U drugim, kao što je Južna Afrika, on je nezavisan od obavještajne službe.

Južnoafrički generalni inspektor za obavještajne službe ima sljedeće primarne odgovornosti nadzora:[25]

- ocjena zakonitosti i učinkovitosti aktivnosti obavještajnih službi; davanje potvrde o zakonitosti operacija obavještajne službe izvršnoj vlasti i građanima Južne Afrike;
- funkcionira kao institucija ombudsmena u pogledu žalbi protiv obavještajnih službi koje podnesu državni službenici i građani.

Nasuprot tome, Belgija (vidjeti Okvir 3), Njemačka (vidjeti Okvir 4), Norveška i Holandija koriste stručna tijela da nadziru svoje obavještajne službe. U pogledu operacija prikupljanja informacija, ta stručna tijela obavljaju sljedeće zadatke:

- osiguravaju da su operacije u skladu sa pravnim okvirom, internim procedurama službe, te politikama izvršne vlasti;
- prate operativnu učinkovitost i daju preporuke za njeno poboljšanje;
- rješavaju žalbe vezane za nezakonito korištenje posebnih istražnih tehnika koje podnesu državni službenici i pripadnici javnosti

Okvir 3: Belgijski stalni odbor za ocjenu obavještajnih agencija

Primjer stručnog nadzornog tijela je Belgijski stalni odbor za ocjenu obavještajnih agencija, koji je uspostavljen Zakonom koji regulira ocjenjivanje policije i obavještajnih službi i koordinacijske jedinice za procjenu prijetnji. Ovaj Odbor ima mandat da nadgleda funkcioniranje dvije obavještajne službe u Belgiji te Koordinacijsku jedinicu za procjenu prijetnji. Nadzor ovog Odbora usmjeren je na zakonitost i učinkovitost aktivnosti obavještajnih službi, kao i na koordinaciju obavještajne i sigurnosne zajednice. Kako bi ispunio ove odgovornosti, Odbor ima ovlast da „istražuje aktivnosti i metode obavještajnih službi“, uključujući načine na koje službe prikupljaju informacije.[26]

Odbor je 2010. godine dobio zadatak da nadzire korištenje novousvojenih intruzivnih metoda prikupljanja informacija obavještajnih službi. Odbor ocjenjuje svaku operaciju tajnog praćenja, te može narediti njeno prekidanje (i uništavanje prikupljenih informacija) ako nisu u skladu sa zakonom.[27] Nadalje, Odbor je ovlašten da rješava žalbe i navode u pogledu rada, intervencije i postupanja obavještajnih službi ili njihovog propuštanja da postupe.”[28]

Okvir 4: Njemačka Komisija G10

Stručno nadzorno tijelo koje prati prikupljanje informacija u Njemačkoj je Komisija G10. Ovu Komisiju čine četiri člana, od kojih je jedan sudija, a može uključiti i parlamentarce. Mada članove Komisije imenuje Parlamentarni kontrolni panel, njihova nezavisnost u radu je zajamčena zakonom. Jedna od njihovih glavnih funkcija je odlučivati da li je korištenje intruzivnih metoda prikupljanja informacija od strane obavještajnih službi dopustivo i potrebno. Prema tome, zakon zahtijeva od Njemačke vlade da obavijesti članove Komisije svakog mjeseca o predstojećim operacijama koje će uključiti intruzivne istražne metode. Ukoliko članovi Komisije izjave da je bilo koja od ovih metoda nepotrebna ili nedopustiva, Vlada mora poništiti saglasnost za te operacije koje je izdala.[29]

Komisija G10 također ima funkciju rješavanja žalbi. Ona može razmotriti žalbe koje se, između ostalog, tiču intruzivnih metoda prikupljanja informacija te odlučiti da li meritum tih žalbi ograničava sposobnost obavještajnih službi da koriste takve metode.[30]

Kako bi bilo učinkovito u nadziranju informacija, stručno nadzorno tijelo mora imati mandat koji mu dozvoljava da djeluje po vlastitoj inicijativi. Ono posebno treba da ima ovlast da provodi istrage na vlastitu inicijativu i ima pristup širokom spektru informacija obavještajnih službi, bilo da su klasificirane ili ne. Zauzvrat, stručno nadzorno tijelo treba da pruži mogućnost osobama koje smatraju da su njihova prava prekršena da mu se obrate. Usto, ono mora pripremati redovne izvještaje parlamentu, a prečišćene verzije ovih izvještaja moraju se učiniti javnim kako bi se promovirala transparentnost.

7. ZAKLJUČAK

U ovom poglavlju razmotrili smo kada i kako obavještajnim službama treba dopustiti da ograniče ljudska prava radi postizanja sigurnosnih ciljeva. Drugim riječima, razmatrali smo pitanje: Kada se državni resursi mogu koristiti da se ograniče prava pojedinaca? Temeljni aspekt ovog pitanja je veza između građana i njihove vlade. Do kojeg god odgovora društvo dođe, strog i jasno definiran sistem davanja saglasnosti i nadzora uvijek je potreban kako bi se osiguralo da obavještajne agencije djeluju unutar zakonskog okvira.

Nadzor nad operacijama prikupljanja informacija je posebno važan zato što u demokratskim zemljama učinkovito prikupljanje obavještajnih informacija zavisi od legitimiteta institucija, dobrog upravljanja i, u krajnjoj instanci, povjerenja javnosti. Ti uslovi mogu se postići samo ako su aktivnosti obavještajnih službi definirane i zasnovane na pravnom okviru koji štiti ljudska prava i prihvata demokratske principe otvorenosti, transparentnosti i odgovornosti. Na tim temeljima, i samo na tim temeljima, može se osigurati legitimno korištenje tajnih, intruzivnih metoda.

8. PREPORUKE

- Dopustivo korištenje istražnih metoda koja ograničavaju ljudska prava, uključujući pravo na privatnost, treba biti jasno definirano u zakonskom okviru unutar kojeg obavještajne službe djeluju.
- U zakonima treba konkretno navesti osnove za korištenje tajnih, intruzivnih metoda prikupljanja informacija, pri čemu treba naglasiti da se takve metode mogu koristiti samo kada su srazmjerne cilju kojem se teži i kada nijedna druga metoda nije dovoljna za ostvarenje cilja.
- Zakonski okvir treba da utvrdi jasne procedure davanja saglasnosti kojom se regulira korištenje tajnih, intruzivnih metoda prikupljanja informacija. Viši stepen intruzivosti treba da zahtijeva i više nivoe saglasnosti.
- Zakonski okvir treba da zahtijeva sudsku saglasnost za korištenje tajnih, intruzivnih metoda prikupljanja informacija u matičnoj državi. Treba također uspostaviti procedure za imenovanje sudija ovlaštenih da daju te saglasnosti i utvrđuju koje kriterije oni treba da koriste u ocjeni zahtjeva za upotrebu intruzivnih metoda.
- Zakonski okvir treba da stvori učinkovite mehanizme nadzora kako bi parlamentarni odbori, stručna nadzorna tijela ili obje ove instance mogle da prate korištenje tajnih, intruzivnih metoda prikupljanja informacija.

Bilješke

1. Vijeće Evrope, Ministarski komitet, *Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism* (20. april 2005), Rec(2005)10, Poglavlje I (dostupno na https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM).
2. Za potpuniju diskusiju o ovoj tački, vidjeti Ronnie Kasrils, "To spy or not to spy? Intelligence and democracy in South Africa," u T*o spy or not to spy? Intelligence and democracy in South Africa*, uredn. Lauren Hutton (Pretoria: Institute for Security Studies, 2009),str. 9–22.
3. Za potpuniju diskusiju o ovoj tački, vidjeti Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States," u *Democratic Control of Intelligence Services: Containing Rogue Elephants*, eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), str. 3–24.
4. Južna Afrika, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10. septembar 2008) (dostupno na http://www.ssronline.org/document_result.cfm?id=3852; pristupljeno 11. juli 2011).
5. Ibid., str.158–159.
6. Vijeće UN-a za ljudska prava, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4. februar 2009), str. 6–7 (dostupno na http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; pristupljeno 14. Februar 2012).
7. Vijeće Evrope, Evropska komisija za demokratiju putem prava (Venecijanska komisija), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007) (dostupno na http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp; pristupljeno 22. oktobra 2011).
8. Južna Afrika, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10. septembar 2008), str. 157 (dostupno na www.ssronline.org/document_result.cfm?id=3852).
9. Evropski parlament, Privremeni odbor za sistem presretanja ECHELON Interception System, *Draft document on the existence of a global system for intercepting private and commercial communications* (ECHELON interception system) (2001) (dostupno na http://cryptome.org/echelon-ep.htm; pristupljeno 16. jula 2011).
10. Vijeće Evrope, Ministarski komitet, Recommendation Rec(2005)10 of the *Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism* (20. april 2005), Rec(2005)10, Poglavlje II (a) (dostupno na https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM; prustupljeno 2. februara 2012).
11. Ibid., Poglavlje II (b) (4).
12. Ibid., Poglavlje II (b) (5).
13. Ibid., Poglavlje II (b) (6).
14. Njemačka, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), *Federal Law Gazette I*, str. 1254, revidirano 2298, posljednji put dopunejno Čl. 1. Zakona od 31. jula 2009, *Federal Law Gazette I*, str. 2499, Čl. 3 (2).
15. Za potpuniju diskusiiju o ovoj tački, vidjeti Gregory Rose i Diana Nestorovska, "Terrorism and National Security Intelligence Laws: Assessing Australian Reforms" in *LAWASIA Journal* (2005), str. 127–155.
16. Vijeće Evrope, Evropska komisija za demokratiju putem prava (Venecijanska komisija), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), str. 44–45 (dostupno na http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp; pristupljeno 22. oktobra 2011).
17. Canada, Security and Intelligence Service Act (31. avgust 2004), R.S.C., 1985, Poglavlje C-23, Čl. 21 (2) (dostupno na http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
18. Argentina, National Intelligence Law, Law 25520 of 2001, Naslov VI, Čl. 18.
19. Website Saveznog pravosudnog centra (Federal Judicial Center), "Foreign Intelligence Surveillance Court" (dostupno na http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html).
20. Južna Afrika, Regulation of Interception of Communications and Provision of Communication-Related Information Act, Zakon br. 70 of 2002, *Government Gazette*, Vol. 451, br. 24286 (22. januar 2003), Čl. 24 (dostupno na www.info.gov.za/gazette/acts/2002/a70-02.pdf; *pristupljeno 2. februara 2012*).
21. Argentina, National Intelligence Law, Law 25520 of 2001, Naslov VI, Čl. 34II.
22. Njemačka, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), *Federal Law Gazette I*, str. 1254, revidirano 2298, posljednji put dopunjeno Čl. 1.

Zakona od 31. jula 2009, *Federal Law Gazette I*, str. 2499, Čl. 14.

23. Ibid., Čl. 5.
24. L. Britt Snyder, *Sharing Secrets with Lawmakers: Congress as a User of Intelligence* (Washington: Central Intelligence Agency, februar 1997) str. 49 (dostupno na https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sharing-secrets-with-lawmakers-congress-as-a-user-of-intelligence/toc.htm; prustupljeno 14. februara 2012).
25. Imtiaz Fazel, "Who shall guard the guards? Civilian oversight and the Inspector General of Intelligence," u *To spy or not to spy? Intelligence and democracy in South Africa*,uredn. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), str. 35–36.
26. Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991); Vidjeti i website belgijskog Standing Intelligence Agencies Review Committee web site (dostupno na www.comiteri.be).
27. Belgija, Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité (4. februar 2010).
28. Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 34.
29. Ibid., Čl. 15.
30. Njemačka, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (June 26, 2001), *Federal Law Gazette I*, str. 1254, revidirano 2298, posljednji put dopunjeno Čl. 1. Zakona od 31. jula 2009, *Federal Law Gazette I*, str. 2499, Čl. 15.

POGLAVLJE 6

Nadzor nad korištenjem ličnih podataka

Ian Leigh

6

Nadzor nad korištenjem ličnih podataka

Ian Leigh

1. UVOD

Ovo poglavlje razmatra načine na koje nadzorna tijela mogu osigurati da obavještajne službe koriste lične podatke u skladu sa zakonom o tim službama. Cilj mu je objasniti ulogu koju nadzorna tijela igraju prilikom provjeravanja kako obavještajne službe pohranjuju, pristupaju i drugima prenose lične podatke. Ne bavi se, međutim, time kako obavještajne službe prikupljaju lične podatke (obuhvaćeno u Poglavlju 5 – Hutton), niti kako se lični podaci razmjenjuju sa domaćim i obavještajnim službama iz inostranstva (obuhvaćeno u Poglavlju 7 – Roach).

Teme koje ovo poglavlje razmatra uključuju: rizike koji nastaju iz korištenja ličnih podataka od strane obavještajnih službi, odgovarajući pravni okvir za reguliranje tog korištenja, te sredstva za nadzor tog korištenja. U zaključku dajemo kratki sažetak ključnih principa za usvajanje zakona o korištenju ličnih podataka od strane obavještajnih službi.

U skladu sa raširenom međunarodnom pravnom praksom, ovo poglavlje će koristiti pojam lični podaci u značenju „svaka informacija koja se odnosi na identificiranog pojedinca ili onog koji se može identificirati ('subjekt podataka' – lice na koga se odnose lični podaci).[1]

2. RIZICI PRILIKOM KORIŠTENJA LIČNIH PODATAKA OD STRANE OBAVJEŠTAJNIH SLUŽBI

Obavještajne i sigurnosne službe imaju legitimne razloge koji su vezani za njihov zakonski mandat da prikupljaju, pohranjuju, obrađuju i otkrivaju lične podatke. Pojedinci na koje se podaci odnose mogu biti legitimni predmet interesa zbog sumnje da su umiješani u špijunažu ili terorizam, na primjer. Potreba za prikupljanjem takvih informacija varira od zemlje do zemlje i od službe do službe te zavisi od toga kako su zakonima precizirani zadaci date službe.

Postoji, međutim, stalna prijetnja prešiokog prikupljanja ličnih podataka. U procesu utvrđivanja, na primjer, da li je osumnjičena osoba uključena u terorističke aktivnosti postoji mogućnost da prikupljene informacije dovedu do negativnog zaključka. Jednostavno rečeno, u takvoj situaciji inicijalno prikupljanje informacija ne može se nazvati nepropisnim. Ali, onda kad služba utvrdi da pojedinac nije umiješan, ona ne smije nastaviti prikupljati informacije o njemu, ili, kako se tvrdi, čak ni zadržati, niti koristiti informacije koje je prikupila. Štaviše, kada se to čini, postoji rizik da će služba pasti u iskušenje da prikuplja informacije o sve širem krugu subjekata – na primjer, prikupljanje podataka o saradnicima osumnjičenog ili organizaciji civilnog društva kojoj on pripada. To može imati negativne posljedice, jer dovodi do toga da pojedinci strahuju od učešća u legitimnim aktivnostima organizacija civilnog društva, kao što su sindikati, separatističke političke partije i grupe za zaštitu okoliša, ili antinuklearne grupe. Također, postoji opća opasnost da lični podaci pohranjeni u dosjeima neke obavještajne službe mogu biti zloupotrijebljeni – od strane zvaničnika u zemljama u tranziciji, na primjer, kako bi se ucjenjivali politički protivnici ili zastrašivali novinari.

Nekad se tvrdi da je puko pohranjivanje, klasifikacija, analiza i čuvanje informacija od strane obavještajnih službi bezazleno. Dok prikupljanje ličnih podataka predstavlja očigledniju prijetnju (vidjeti Poglavlje 5 – Hutton), njihovo pohranjivanje je potencijalno štetno zato što su lični podaci tijesno povezani sa ličnom autonomijom. Kontrola koju pojedinci imaju nad vlastitim životom – osobito izbori koje oni čine u pogledu pojedinosti iz ličnog života (kome, u kojoj mjeri i u koju svrhu odlučuju da ih otkriju), podriva se kada vladine agencije imaju dozvolu da prikupljaju lične podatke iz različitih izvora.

Gomilanjem ličnih podatka o pojedincima, obavještajne službe imaju izvjesnu kontrolu nad subjektima tih informacija. U najgorim slučajevima, lični podaci koje čuvaju službe mogu se koristiti nepropisno kako bi se izvršio pritisak na političare ili novinare, na primjer. Čak i spoznaja da službe čuvaju njihove lične podatke može biti psihološki uznemirujuća za te pojedince, čak i ako se nikada ne desi štetno razotkrivanje tih podatka. Slično, učešće u aktivnostima civilnog društva može biti umanjeno zbog spoznaje (ili neodagnane sumnje) da se informacije o određenim oblicima političkog, industrijskog ili društvenog aktivizma čuvaju u sigurnosnim dosjeima.

S obzirom na često spominjanu potrebu da se sigurnosne informacije čuvaju na duže vremenske periode, mogućnost da im učine štetu može utjecati na pojedince godinama ili decenijama. Informacije vezane za mladenačke aktivnosti neke osobe, na primjer, mogu u nekim slučajevima biti čuvane dok ta osoba ne zađe u starost, čak i ako njegov ili njen kasniji život ne daje nikakvog razloga da se tretira kao sigurnosni rizik.

Nadalje, lični podaci koje čuvaju obavještajne službe mogu biti pristrasni, neprecizni ili zastarjeli. U ekstremnim slučajevima, mogu čak biti pribavljeni iz izvora sa željom da se učini šteta datoj osobi iz ličnog animoziteta ili ljubomore. Slično, doušnici motivirani novčanom nagradom mogu biti potaknuti da preuveličavaju ili "naštimavaju" činjenice o ljudima o kojima služba prikuplja informacije.

Ostali rizici vezani za pohranjivanje ličnih podatka uključuju dosad neviđenu sposobnost nekih obavještajnih službi da, zahvaljujući privilegiranom pristupu informacijama, povezuju podatke o pojedincima, koji se inače nalaze u različitim bazama podataka organa za provedbu zakona, zdravstvenih ustanova i poreznih službi.

Rizici, naravno, ne završavaju sa pohranjivanjem, klasifikacijom i analizom ličnih podataka. Postoje i rizici koji su vezani za njihovo korištenje. Neki vidovi korištenja su legitimni (kao što je sigurnosna provjera), dok su drugi manje prihvatljiva (kao što je rasno ili religijsko profiliranje ili vršenje prikrivenog utjecaja na osobu). Neovlašteno otkrivanje ličnih podataka medijima, na primjer, može pojedincu na kojeg se ta informacija odnosi učiniti štetu ili dovesti do gubitka životnih prilika. Lični status osobe može biti pogođen, na primjer, kada se podvrgne sigurnosnoj provjeri i bude ocjenjena negativno, ili kada joj se oduzme prethodna pozitivno ocijenjena sigurnosna provjera; i, općenitije, reputacija osobe može biti oštećena. Slično tome, otkrivanje nepotkrijepljenih ili netačnih podataka stranim vladama može rezultirati ukidanjem mogućnosti putovanja ili još gorim ishodima (vidjeti Roach – Poglavlje 7).

Obavještajne službe imaju veliki interes da se staraju da informacije o subjektima koje čuvaju budu pravične, tačne i ažurirane. Učinkovitost službe i njena reputacija mogu biti negativno pogođeni ako ona razotkrije, daje savjete ili djeluje na osnovu pogrešnih, nepotpunih ili zastarjelih informacija. Ipak, postoje izvjesni rizici svojstveni obavještajnom radu koji nalažu jače razloge za vanjsku kontrolu i nadzor nad procedurama rukovanja informacijama. Osobito, pritisak kojem su izložene službe da predviđaju buduće sigurnosne rizike može ih poticati na preširoko prikupljanje informacija o sve većem broju pojedinaca. Tehnološke promjene, kao što su poboljšanja u traganju za podacima, mogu jednako tako ohrabriti službe da prikupljaju i pohranjuju ogromne količine ličnih informacija – npr. podatke o porukama elektronske pošte, pretraživanju internet stranica, rezervacijama avionskih karata i finansijskim transakcijama.

3. PRAVNI OKVIR ZA KORIŠTENJE LIČNIH PODATAKA OD STRANE OBAVJEŠTAJNIH SLUŽBI

Pravo na privatnost je zaštićeno zakonom o ljudskim pravima kako je to utvrđeno u glavnim međunarodnim ugovorima.[2] Iz razloga relevantnosti i praktičnosti, međutim, ovo poglavlje će se usredsrediti na standarde ljudskih prava primjenjive u Evropi, pogotovo onim koji su utvrđeni u Evropskoj konvenciji o ljudskim pravima (ECHR) a koji su istovremeno i najrazvijeniji. Mada je ovo poglavlje je usredsređeno na pravo na privatnost, prikupljanje i korištenje ličnih podataka od strane obavještajnih službi, ono može indirektno utjecati i na druga ljudska prava, kao što su prava na slobodu izražavanja i slobodu udruživanja.

Član 8. ECHR-a, koja se primjenjuje u četrdeset i sedam država-članica Vijeća Evrope, navodi:

> *1. Svako ima pravo na poštivanje svog privatnog i porodičnog života, doma i prepiske.* [Evropski sud za ljudska prava (ECtHR) tumači ovu odredbu tako da uključuje telefonske pozive i ostala sredstva za elektronsko komuniciranje.]
>
> *2. Javna vlast ne smije da se miješa u vršenje ovog prava, osim ako je takvo miješanje predviđeno zakonom i ako je to neophodna mjera u demokratskom društvu u interesu državne sigurnosti, javne sigurnosti, ekonomske dobrobiti zemlje, sprječavanja nereda ili sprječavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih.*

Povelja o temeljnim pravima Evropske unije također je važna stoga što sadrži eksplicitne odredbe za zaštitu ličnih podataka koje su obavezujuće za države članice Evropske unije (EU). Njen Član 8. glasi:

> *1. Svako ima pravo na zaštitu ličnih podataka koja se njega ili nje tiču.*
>
> *2. Takvi podaci moraju biti obrađeni pravično za specifično navedene svrhe i na osnovu saglasnosti date osobe ili nekoj drugoj legitimnoj osnovi koja je utvrđena zakonom. Svako ima pravo da pristupi podacima koji su prikupljeni u vezi sa njim ili njom, i ima pravo da se oni isprave.*
>
> *3. Poštivanje ovih pravila će biti predmet kontrole nezavisnog organa.*

Nadalje, prema Članu 52.1. Povelje:

> *Svako ograničavanje u uživanju prava i sloboda priznatih ovom Poveljom mora biti utvrđeno zakonom i mora poštovati suštinu tih prava i sloboda. U skladu sa principom proporcionalnosti, ograničenja se mogu nametnuti samo ako su potrebna i ako istinski ispunjavaju ciljeve od općeg interesa priznata od same Unije ili potrebe za zaštitom prava i sloboda drugih.*

Međutim, pošto ove odredbe Povelje o temeljnim pravima još nisu ishodile nikakvu sudsku praksu, ovaj tekst će se prvenstveno usredsrediti na ECHR.

ECtHR je ustanovio da vladini sigurnosni dosjei koji sadrže lične podatke jasno potpadaju pod okvir zaštićenog privatnog života, kako je to utvrđeno u Članu 8.ECHR-a. Sud je također u nekoliko slučajeva utvrdio da prikupljanje, pohranjivanje i otkrivanje ličnih podataka od strane obavještajne službe predstavlja „miješanje“ u pravo na poštivanje privatnog života – što je dopustivo samo po strogim kriterijima utvrđenim u Članu 8.2. Nalazi Suda primjenjuju se ne samo na otkrivanje informacija drugim vladinim agencijama, već i na njihovo korištenje za internu sigurnosnu provjeru.[3] U odlučivanju u predmetu *Rotaru protiv Rumunije* (2000), koji se odnosi na sigurnosne dosjee koje su držale rumunske obavještajne službe, Sud je ustanovio da:

> *i pohranjivanje, od strane javnog organa, informacija vezanih za privatni život pojedinca i njihovo korištenje te odbijanje da se pruži prilika da se te informacije opovrgnu, predstavlja miješanje u pravo na poštivanje privatnog života, zajamčeno Članom 8.1. Konvencije.*[4]

3.1 DOPUSTIVA OGRANIČENJA PRAVA NA PRIVATNOST

Kako bi pohranjivanje i korištenje ličnih podataka obavještajne službe bilo u skladu sa ECHR, ono mora zadovoljiti kriterije utvrđene u Članu 8.2. To znači, da to korištenje mora biti „u skladu sa zakonom“, „potrebno u demokratskom društvu“ i „u interesu sigurnosti države“.

Test za „u skladu sa zakonom“ nameće strogi kriterij. Ako taj kriterij ne može biti ispunjen, dolazi do kršenja Člana 8, bez obzira na šire interese koji su u pitanju u datom slučaju. Tako, zahtjev legalnosti nameće parlamentarcima obavezu da utvrde dobar zakonski osnov za korištenje ličnih podataka od strane obavještajnih službi.

ECtHR tumači pojam „u skladu sa zakonom“ tako da znači da svako ograničenje prava na privatnost treba da ima „neki osnov u domaćem zakonu“ i da ispunjava test „kvaliteta zakona“, što je Sud definirao kao „dostupno datoj osobi, koja, štaviše, mora biti u stanju predvidjeti konsekvence koje to može imati za nju, te [mora biti] u skladu sa vladavinom prava.”[5]

Primjenjujući te testove, ECtHR je ustanovio kršenje Člana 8. tamo gdje ne postoji zakon kojim bi se rukovodile obavještajne službe ili tamo gdje takav zakon postoji, ali ne uključuje odredbe koje reguliraju prikupljanje i pohranjivanje ličnih podataka.[6] Nadalje, pod testom „kvaliteta zakona“, takav zakon „mora biti dovoljno jasan u svojim odredbama da građanima daje adekvatnu indikaciju u pogledu okolnosti u kojima [zakon može biti korišten].”[7] Usto, pošto „praktična provedba mjera tajnog nadzora komunikacija nije podložna kontroli datog pojedinca ili javnosti općenito“, zakonima koji reguliraju prikupljanje ličnih podataka ne smije se dopustiti „da se izvršnoj vlasti ili sudiji da diskreciono pravo koje bi bilo izraženo u kategorijama neograničene moći” i, prema tome, mora se „dati indikacija koliko je to dato diskreciono pravo… i na koji se način ono provodi i to dovoljno jasno da pojedincu pruži adekvatnu zaštitu od proizvoljnog miješanja.”[8]

U razmatranju tih zakona, sud provjerava da li oni dovoljno jasno navode, između ostalog, procedure koje treba primijeniti radi provjere korištenja i pohranjivanja prikupljenih podataka; predostrožnosti koje treba preduzeti kada se ti podaci prenose drugim stranama; i okolnosti u kojima snimci koji su dobiveni praćenjem mogu ili moraju biti uništeni.[9]

Nedavni slučaj koji se tiče Vlade Rusije ilustrira ove principe.[10] Sud je ustanovio da registracija jednog aktiviste za ljudska prava u bazi podataka tajnog nadzora predstavlja kršenje Člana 8. ECHR-a. Pošto je baza podataka stvorena na osnovu neobjavljene naredbe ministra, koja nije bila dostupna javnosti, javnost nije mogla znati zašto su određeni pojedinci registrirani u toj bazi podataka, koji tip informacija je pohranjivan, kako su bile pohranjivane, koliko dugo će ostati pohranjene, kako će biti korištene i ko će imati kontrolu nad tim.

Test „kvaliteta zakona“ ne uzima u obzir, međutim, legitimna sigurnosna pitanja. U kontekstu sigurnosne provjere, na primjer, dio testa koji se odnosi na „predvidljivost“ ne nalaže da se podnosiocima zahtjeva omogući da predvide proces u potpunosti (jer bi inače proces mogao biti lako zaobiđen). Umjesto toga, važeći zakon treba samo pružiti uopćeni opis date prakse.[10]

Okvir 1: Test "kvaliteta zakona" u praksi

U slučaju *Rotaru protiv Rumunije*[12] Evropski sud za ljudska prava razmotrio je rumunski Zakon o reguliranju sigurnosnih dosjea koje čuva Vlada. Sud je utvrdio da je Zakon nedovoljno jasan u pogledu opisa okolnosti u kojima se može primijeniti – posebno u pogledu kako se mogu koristiti lične informacije sadržane u dosjeima – niti Zakon utvrđuje bilo kakav mehanizam za praćenje korištenja informacija.

Sud je također ustanovio da je Zakon neadekvatan zato što ne sadrži „indikaciju" koja bi bila dovoljno jasna u pogledu opsega diskrecionog prava datog Vladi Rumunije. Drugim riječima, Zakon nije uspio ograničiti provođenje ovlasti vlade u pogledu prikupljanja, bilježenja i arhiviranja ličnih informacija u tajne dosjee. Posebno, Zakon nije definirao vrstu informacija koja se može snimati, kategorije ljudi protiv kojih se mogu poduzeti mjere nadzora, okolnosti u kojima takve mjere mogu biti poduzete, te procedure kojih se treba pridržavati. Zakon nije uključio nikakva ograničenja u pogledu vremenskog trajanja čuvanja informacija.[13]

U pogledu sigurnosnih arhiva koje su čuvale obavještajne službe prije revolucije, Zakon dopušta da se ostvari uvid u te arhive, ali ne sadrži „jasne, detaljne odredbe u pogledu osoba kojim je dopušten uvid u dosjee, prirodu tih dosjea, procedure kojih se treba pridržavati, ili moguće korištenje informacija prikupljenih na taj način."[14]

Kada zakon ispuni kriterij „kvalitet zakona" u pogledu jasnoće, dostupnosti i predvidljivosti, ECHR zahtijeva provjeru svrhe i potrebe miješanja u privatni život. To podrazumijeva procjenu proporcionalnosti – to jest, da li je miješanje pretjerano, čak i kad se uzme u obzir legitimni cilj zaštite državne sigurnosti. Na primjer, u jednom nedavnom slučaju, ECHR je ustanovio da je Švedska vlada prekršila Član 8. ECHR-a kada je sačuvala lične podatke u sigurnosnom dosjeu u periodu dužem od trideset godina. U pogledu prirode i starosti tih informacija, Sud nije prihvatio argument odbrane da su iza odluke o produženju čuvanja informacija stajali relevantni i dovoljni razlozi državne sigurnosti.[15]

U razmatranju pitanja da li je miješanje u privatni život „potrebno u demokratskom društvu", „Sud uzima u obzir garancije koje su ustanovljene kako bi se nadziralo pohranjivanje i korištenje ličnih podataka – posebno onih koji se tiču nezavisnih tijela.[16] Tamo gdje ne postoje garancije koje bi omogućile osobama da zaštite svoje pravo na privatan život, Sud utvrđuje da je došlo do kršenja Člana 8. U predmetu *Turek protiv Slovačke* (2006), na primjer – u kojem se aplikant žalio da je registriran kao saradnik bivše čehoslovačke komunističke sigurnosne agencije, da je bio podvrgnut sigurnosnoj provjeri te da mu je odbijen zahtjev u kojem je osporio tu registraciju – Sud je utvrdio da nepostojanje procedure kojom bi aplikant mogao tražiti zaštitu svog prava na privatni život predstavlja kršenje Člana 8.[17]

Čak i kada takve procedure postoje u zakonu, pretjerano kašnjenje u pružanju odgovora na zahtjev pripadnika javnosti da dobiju pristup informacijama o sebi može se smatrati kršenjem zakona (zato što garancije nisu učinkovite). Na primjer, u predmetu *Haralambie protiv Rumunije* (2009), Sud je ustanovio da je šestogodišnje odlaganje Vlade Rumunije da dozvoli aplikantu pristup njegovom ličnom sigurnosnom dosjeu, koji je nastao u prethodnom komunističkom režimu, predstavlja kršenje njegovog prava iz Člana 8. ECHR-a.[18]

Postoji potreba za jasnim zakonskim ograničenjima u pogledu prikupljanja i korištenja

ličnih podataka, kao i za tim da nadzorna tijela osiguraju da se službe pridržavaju zakonâ koji reguliraju upravljanje takvim podacima. Specijalni izvjestilac UN-a za promociju i zaštitu ljudskih prava i temeljnih sloboda prilikom borbe protiv terorizma potvrdio je tu potrebu u svom izvještaju Vijeću za ljudska prava Ujedinjenih nacija 2010. godine:

> *Javno dostupni zakoni utvrđuju tipove ličnih podataka koje obavještajne službe mogu čuvati i kriterije koji se primjenjuju u pogledu korištenja, čuvanja, brisanja i otkrivanja tih podataka. Obavještajnim službama je dopušteno da čuvaju lične podatke koji su potrebni isključivo u svrhu izvršavanja njihovog mandata.*[19]

3.2 PRINCIPI ZAŠTITE PODATAKA

Konvencija Vijeća Evrope o zaštiti pojedinaca u pogledu automatske obrade ličnih podataka[20] ("Konvencija o zaštiti podataka") utvrđuje minimum principa za države članice na polju zaštite podataka (vidjeti Tabelu 1). Prema Konvenciji o zaštiti podataka, svaka država potpisnica preuzima na sebe obavezu da „preduzme potrebne mjere u svom domaćem zakonodavstvu kako bi ispoštovala osnovne principe zaštite podataka "[21] te da „ustanovi odgovarajuće sankcije i pravne lijekove za kršenje odredbi domaćeg zakona kojim se poštuju osnovni principi zaštite podataka."[22] Usto, neki aspekti ovih principa – posebno oni koji su vezani za pravično suđenje, davanje saglasnosti, zakonsko ovlaštenje, pristup subjekta i ispravku – mogu se naći u Članu 8.2. Povelje o temeljnim pravima Evropske unije.

TABELA 1: PRINCIPI VIJEĆA EVROPE O ZAŠTITI PODATAKA

Princip zaštite podataka	Zahtjevi
Kvalitet podataka (Član 5)	Lični podaci koji su podvrgnuti automatskoj obradi bit će: a. dobiveni i obrađeni pravično i zakonito; b. pohranjeni za specifične i legitimne svrhe i neće biti korišteni na način koji nije kompatibilan sa tim svrhama; c. adekvatni, relevantni i neće biti pretjerani u vezi sa svrhom zbog koje se pohranjuju; d. precizni i, tamo gdje je potrebno, ažurirani; e. sačuvani u obliku koji dozvoljava identifikaciju subjekata podatka ne duže nego što je to potrebno za svrhu u koju su ti podaci pohranjeni.
Sigurnost podataka (Član 7)	Odgovarajuće sigurnosne mjere će biti poduzete radi zaštite ličnih podataka pohranjenih u automatiziranim bazama podataka protiv slučajnog ili neovlaštenog uništavanja, slučajnog gubitka, kao i neovlaštenog pristupa, mijenjanja ili diseminacije.
Pravo da se utvrdi postojanje ličnih podataka (Član 8)	Svaka osoba će imati mogućnost: da utvrdi postojanje automatiziranog dosjea sa ličnim podacima, njegove glavne svrhe, kao i identitet i uobičajeno boravište ili glavno sjedište onog koji kontrolira taj dosje.
Pravo pristupa (Član 8)	Svaka osoba će imati mogućnost: ▪ dobiti u razumnom roku i bez pretjeranog kašnjenja ili troška potvrdu da li su lični podaci koji se na njega odnose pohranjeni u automatiziranu bazu podataka, kao i to da će mu biti preneseni takvi podaci u čitljivom obliku. ▪ dobiti, ako je takav slučaj, ispravku ili brisanje takvih podataka ako su obrađeni suprotno odredbama domaćeg zakona kojim se poštuju temeljni principi utvrđeni u Članovima 5. i 6. ove Konvencije.
Pravo na pravni lijek (Član 8)	Svaka osoba će imati mogućnost: da ima pravni lijek ako njen zahtjev za potvrdom ili, kao što može biti slučaj, komunikacijom, ispravkom ili brisanjem, kao što se to navodi u stavovima b) i c) ovog Člana, nije ispoštovan.

Konvencija o zaštiti podataka (Član 11) navodi da su principi koji su u njoj sadržani osmišljeni kao minimalni standardi, pri čemu se mogu dopuniti širim mjerama zaštite.

Način na koji Konvencija o zaštiti podataka definira ograničenja u vezi sa principima zaštite podataka slični su načinu na koji ECHR definira ograničenja prava na privatnost (koja su ranije razmatrana). Ograničenja moraju biti „utvrđena zakonom [države potpisnice]" te moraju predstavljati „potrebnu mjeru u demokratskom društvu "[23] radi zaštite legitimnog interesa, kao što je državna sigurnost ili pravo subjekta čiji se podaci čuvaju.[24]

3.3 RELEVANTNOST DOMAĆEG ZAKONODAVSTVA

Pošto prikupljanje, upravljanje i otkrivanje ličnih podataka od strane obavještajnih službi može izazvati potencijalno ozbiljne štete po ljudska prava, ispravno je da smjernice za upravljanje i korištenje takvim podacima budu demokratski utvrđene u zakonu koji je dostupan javnosti. Ta praksa ima nekoliko prednosti: ohrabruje političku debatu o opsegu aktivnosti obavještajne službe, oduzima službi ili izvršnoj vlasti diskreciono pravo odlučivanja, te daje službi jasan mandat u odnosu na njene radnje koje mogu kršiti ljudska prava.

Zakoni koji reguliraju korištenje ličnih podataka od strane obavještajnih službi mogu se odnositi na jednu ili više sljedećih tema:

- dopustivi i nedopustivi razlozi za obradu ličnih podataka;
- ograničenja u pogledu otkrivanja ličnih podataka;
- javno otkrivanje tipova podataka koji su pohranjeni;
- pristup ličnim podacima od strane subjekta podataka;
- obavještenje da su prikupljeni lični podaci;
- pregled, revizija, i brisanje ličnih podataka.

3.3.1 Dopustivi i nedopustivi razlozi za obradu ličnih podataka

Zakoni ove vrste mogu specificirati tipove ličnih podataka koji se mogu prikupljati i čuvati, kao i to kada dosje koji sadrži lične podatke može biti otvoren (vidjeti Okvir 2). Prepoznajući jasno princip proporcionalnosti, relevantni zakon u Njemačkoj vezuje potrebu za prikupljanjem podataka sa ozbiljnošću odgovarajuće prijetnje. On posebno zahtijeva od domaće obavještajne službe Njemačke (Saveznog ureda za zaštitu Ustava) da razmotri da li željena informacija može biti pribavljena iz otvorenih izvora ili korištenjem sredstava koja manje krše pravo na privatnost.[25] Takvi zakoni mogu također smanjiti vjerovatnoću da će obavještajne službe kršiti ljudska prava time što zabranjuju određene oblike ponašanja službi, kao što je odabir pojedinaca za sigurnosnu obradu samo na osnovu rasnih ili religijskih karakteristika, ili političkih gledišta.

Okvir 2: Ograničenja za obradu ličnih podataka u odabranim jurisdikcijama

Ovaj okvir sadrži odredbe Holandskog i Argentinskog zakona koji ograničavaju obradu ličnih podataka od strane obavještajnih službi na osnovu nedopustivih kriterija.

Holandija[26]

"Glavna obavještajna i sigurnosna služba može obrađivati samo lične podatke koji su vezani za osobe:

a. za koje postoji ozbiljna sumnja da predstavljaju prijetnju za demokratski pravni sistem, ili za sigurnost, ili druge vitalne interese države;
b. koji su dali dozvolu za obavljanje sigurnosne provjere nad njima;
c. za koga je to potrebno u kontekstu istraga vezanih za druge zemlje;
d. o kome je informacije pribavila druga obavještajna ili sigurnosna služba;
e. čiji podaci su potrebni radi podrške ispravnom obavljanju dužnosti službe;
f. koji su trenutno ili su bili zaposleni u službi;
g. u vezi sa kojim je to potrebno u kontekstu provođenja analize prijetnje i rizika, kao što se to navodi u Članu 6, drugi stav, pod e."

Argentina[27]

"Nijedna obavještajna agencija neće… čuvati podatke o pojedincima zbog njihove rase, religije, privatnih radnji i političke ideologije, ili zbog njihovog članstva u partijskoj, društvenoj, sindikalnoj zajednici, zadruzi, pomoći, kulturnim ili radnim organizacijama, ili zbog zakonitih aktivnosti koje se obavljaju u bilo kojem području."

3.3.2 Ograničenja u pogledu otkrivanja ličnih podataka

Pravna ograničenja u pogledu otkrivanja ličnih podataka su općenito poželjna, posebno radi sprječavanja curenja informacija iz partijsko-političkih razloga. Ograničenja ove vrste su posebno važna u zemljama u tranziciji, gdje delikatni zadatak izgradnje povjerenja u neutralnost sigurnosnih institucija može biti ozbiljno podriven ponašanjem koje je partijski obojeno. Mnoge zemlje su uvele krivičnu odgovornost za obavještajne službenike koji odaju informacije sadržane u dosjeima njihove službe, uključujući lične podatke, bez zakonskog ovlaštenja ili u neodobrenu svrhu (vidjeti Okvir 3).

Okvir 3: Zabrana nepropisnog otkrivanja ličnih podataka u Rumuniji

Ova odredba zakona Rumunije ilustrira kako lični podaci mogu biti zaštićeni od nepropisnog otkrivanja od strane obavještajnih službenika:

"Informacije vezane za privatni život, čast ili reputaciju osobe, koje su se slučajno saznale prilikom dobivanja podataka potrebnih za državnu sigurnost, ne smiju se objaviti. Otkrivanje ili korištenje, mimo zakonskog okvira, informacija i podataka navedenih u stavu 1. od strane službenika obavještajnih službi smatra se krivičnim djelom i kažnjivo je zatvorskom kaznom u trajanju od 2 do 7 godina."[28]

3.3.3 Objavljivanje tipova pohranjenih podataka

Zakon o zaštiti podatka u nekim zemljama zahtijeva od državnih agencija, kao što su obavještajne službe, da objavljuju detalje o tipovima ličnih podataka koje čuvaju, svrhu zbog kojih se ti podaci mogu objaviti, opis baza podataka u kojima se oni čuvaju, te uslove i kontrole primjenjive na te baze podataka. Objavljivanje ovih informacija pomaže jačanju transparentnosti i odgovornosti. Pojedinci koji žele ostvariti pravo pristupa i ispravke mogu saznati iz ovih informacija koje državne agencije čuvaju njihove lične podatke, kao i opseg i razloge za čuvanje tih podataka.

U principu, nametanje dužnosti obavještajnim službama da omoguće uvid u lične podatke koje čuvaju je poželjno zato što pomaže jačanju legitimnosti agencija, dok istovremeno otklanja mogućnost neosnovanih spekulacija o njihovom radu. Ovo je korisno čak i tamo gdje postoji dobar razlog koji se tiče državne sigurnosti da se spriječi pojedinac u tome da sazna da li se njegovi lični podaci čuvaju u nekoj obavještajnoj agenciji – na primjer, gdje bi bilo opravdano da odgovor na zahtjev subjekta da dobije pristup tim podacima bude „ni potvrdan, ni odričan“.

Okvir 4: Dužnost da se otkriju informacije u vezi sa bankama podataka prema zakonu Kanade

Ova odredba Kanadskog zakona ilustrira općenitu dužnost da se objave informacije o bazama podataka ličnih informacija:

> “Šef vladine institucije je zadužen da se postara da u banke ličnih informacija budu uključene sve lične informacije pod kontrolom vladinih institucija, koje su (a) korištene, ili se koriste, ili su dostupne za korištenje u administrativnu svrhu; ili (b)su organizirane, ili se namjeravaju tražiti u bazi podataka na osnovu imena pojedinca ili identifikacijskog broja, simbola ili druge pojedinosti pripisane datom pojedincu.”[29]

3.3.4 Pristup subjekta čuvanja podataka njegovim ličnim podacima

Mnoge zemlje su usvojile zakon o zaštiti podataka ili privatnosti koji priznaju pravo subjekata podataka da pristupe ličnim podacima o sebi koje čuvaju vladine agencije (vidjeti Okvir 5). Neki zakoni o zaštiti podataka dodatno priznaju pravo subjekta da ispravi takve informacije, da se u njih unese izjava koja sadrži informacije kojima se osporava tečnost, ili da takve informacije budu uništene. Iz razloga državne sigurnosti, ti zakoni uvijek uključuju specijalne odredbe za podatke koje čuvaju obavještajne službe. Te odredbe imaju različite oblike

Okvir 5: Pravo pristupa ličnim podacima koje čuvaju obavještajne službe po holandskom zakonu

Ove odredbe holandskog zakona ilustriraju kvalificirano pravo subjekta da pristupi ličnim podacima koje čuvaju obavještajne službe:[30]

"Član 47.

1. Nadležni ministar će obavijestiti svaku osobu na njegov/njen zahtjev što je moguće prije, a najkasnije u roku od tri mjeseca, da li se i, ako jeste, koji lični podaci vezani za tu osobu obrađuju u udatoj službi ili u njeno ime."

"Član 48.

1. Osoba koja je u skladu sa Članom 47. provjerila informacije o sebi koju je obradila data služba, ili je obrađena u ime te službe, može o tome dostaviti pisanu izjavu. Ta izjava će biti dodana relevantnim informacijama."

"Član 53.

1. Zahtjev iz Člana 47. će u svakom slučaju biti odbačen ako su:
    a. u kontekstu bilo koje istrage obrađene informacije vezane za osobu koja podnosi zahtjev, osim ako:
        i. su relevantne informacije obrađene prije više od 5 godina,
        ii. 2º. od tada u vezi sa osobom koja podnosi zahtjev nisu bile obrađivane nove informacije u vezi sa istragom u odnosu na koju su relevantne informacije bile obrađene, te ukoliko date informacije nisu relevantne za bilo koju tekuću istragu;
    b. nikakve informacije nisu obrađene u vezi sa osobom koja je podnijela zahtjev."

U nekim zemljama ove službe imaju pravo *izuzeća* od primjene zakona o zaštiti podataka koji se jednostavno ne primjenjuje na informacije u njihovom posjedu. U takvim slučajevima, ne postoji pravo subjekta da pristupi tim informacijama. Ovakav pristup ima prednost zbog svoje jednostavnosti, ali se može smatrati preširokim zbog toga što izuzeća oslobađaju date službe bilo kakve obaveze da objašnjavaju kako se pitanja državne sigurnosti koriste kao opravdanje za čuvanje određenih podataka. Ovaj pristup može također spriječiti djelovanje normalnog vanjskog nadzora i kontrole –recimo, ograničavanjem nadležnosti povjerenika za privatnost.

Jedna varijacija ovog pristupa je izuzeće obavještajnih službi od primjene zakona o slobodi informacija. U tim slučajevima, zakon o zaštiti podataka (uključujući pravo subjekta na pristup vlastitim podacima) i dalje se primjenjuje, barem principijelno, mada je u praksi podložan reviziji, zavisno od pojedinačnog slučaja.

Druge zemlje, opet, u zakon o zaštiti podataka uvele su *izuzetke* na osnovu državne sigurnosti. To su uža i specifičnija izuzeća, zato što na obavještajnu ili sigurnosnu službu prebacuju teret opravdavanja - i to od slučaja do slučaja – zašto se ne mora primijeniti obaveza zaštite prava nekog pojedinca koja proizlaze iz zakona o zaštiti podataka.

Takvi zakoni mogu pojedincima pružiti *prima facie* pravo pristupa vlastitim informacijama, koje se ostvaruje jednostavnim podnošenjem zahtjeva izvršnom nadzornom tijelu, mada

je i to pravo podložno ograničenjima koja za cilj imaju zaštitu tekućih istraga, izvora i metoda.[31] (Sva ova ograničenja treba da budu u skladu sa važećim zakonom, srazmjerna prijetnji, te podložna nezavisnoj ocjeni.[32]). Neovisno od ljudskih prava koja su ovdje u pitanju, ovakav pristup može djelovati kao garancija zaštite od pogrešnog upravljanja i korupcije.

Obično, ovakvi izuzeci omogućavaju službi da pruži odgovor koji nije „ni potvrdan, ni odričan" kako bi se ljudi odvratili od podnošenja spekulativnih zahtjeva, čija je namjera utvrditi koliko informacija data služba uopće čuva.

U praksi, primjena izuzetaka može rezultirati odbijanjem većine zahtjeva. Stoga, rezultat pristupa koji se zasniva na izuzecima može se malo razlikovati od ishoda pristupa koji se zasniva na izuzećima. Tu postoji, međutim, jedna važna distinkcija: pristup koji podrazumijeva izuzetke zahtijeva od agencije da opravda odbijanje otkrivanja informacije u odnosu na zakonsku pretpostavku koja daje prednost otkrivanju, dok pristup izuzeća to ne čini. Dodatno, zahtjev za izuzetkom je podložan ocjeni nezavisnog organa na način na koji zahtjev za izuzećem to nije. Empirijsko istraživanje provedbe kanadskog Zakona o pristupu informacijama iz 1982. i kanadskog Zakona o privatnosti iz 1982. godine, potvrđuje korisnost podvrgavanja procesa rukovanja informacijama u obavještajnim službama vanjskoj kontroli nezavisnog tijela i to ne u najmanjoj mjeri, zato što se time stimulira interna svijest o pitanjima koja se tiču informacija i privatnosti.[33]

Jedna od varijacija je definirati samo određene banke podataka kao „izuzete", čime se one principijelno podvrgavaju različitim nadzornim mehanizmima, dok se u praksi obavještajna služba na taj način oslobađa dužnosti da detaljno odgovori na pojedinačne zahtjeve. Kanada koristi ovaj model kao komplementaran pristupu izuzeća.

Jedno od rešenja je i da važeći zakon može dati ovlast ministru, što je podložno ocjeni, da izda blanko certifikat o izuzeću (kao što je to utvrđeno u Zakonu o zaštiti podatka Ujedinjenog Kraljevstva[34]). Taj pristup pruža velike garancije za obavještajne službe da njihovi podaci neće biti otkriveni na način koji je, na primjer, u suprotnosti sa zaštitama garantiranim partnerskim službama ili doušnicima. S druge strane, takve potvrde su obično preširoke, čime se uklanja vanjska kontrola i koristi koje ona nosi, uključujući povjerenje javnosti u propisan rad službe. Opravdana zabrinutost u pogledu sigurnosnih informacija se bolje rješava specifičnim izuzecima umjesto blanko izuzeća. Štaviše, pored mogućnosti pristupa subjekta i ispravke, principi zaštite podataka vezani za kvalitet podataka i sigurnost podataka su očito relevantni za obavještajne službe te stoga predstavljaju daljnje razloge da se službe ne izuzimaju iz nadležnosti zakona o zaštiti podataka.

Okvir 6: Pristup ličnim podacima koje čuvaju obavještajne službe: dobre prakse koje je identificirao specijalni izvjestilac UN-a

"Pojedinci imaju mogućnost da zahtijevaju pristup svojim ličnim podacima koje čuvaju obavještajne službe. Pojedinci mogu to pravo ostvariti tako što će uputiti zahtjev nadležnom organu ili putem nezavisne institucije za zaštitu podataka ili nadzor. Pojedinci imaju pravo ispraviti netačnosti u svojim ličnim podacima. Svaki izuzetak od ovih općih pravila propisan je zakonom i strogo ograničen, proporcionalan i potreban radi ispunjavanja mandata obavještajne službe. Obaveza obavještajne službe je da opravda nezavisnoj instituciji za nadzor svaku svoju odluku da ne otkrije lične informacije."[35]

3.3.5 Obavještenje o prikupljenim ličnim podacima

Neke zemlje (poput Holandije[36] i Njemačke[37]) zahtijevaju da subjekti prikupljanja ličnih podataka (posebno putem nadzora) budu naknadno obaviješteni da su informacije o njima prikupljane (vidjeti Okvir 7). U teoriji, ova praksa omogućava retrospektivno osporavanje, te nameće provjeru odluke obavještajne službe da otvori dosje o subjektu. Međutim, ograničenja koja se nameću na pravo na to da se bude obaviješten kako bi se zaštitile tekuće operacije i identitet izvorâ mogu to pravo u mnogim slučajevima svesti na puku iluziju. Iz tog razloga, ova praksa je trenutno predmet revizije u Holandiji.[38]

Tamo gdje nema prava na obavještavanje ili ispravku, rizici za korištenje ličnih podataka od strane obavještajnih službi neizbježno su veći, a potreba za drugim kontrolama je u skladu s tim veća.

Okvir 7: Dužnost da se obavijeste subjekti čuvanja podataka po njemačkom zakonu

Ove odredbe njemačkog zakona ilustriraju princip obavještavanja:

"Subjekt čuvanja podataka će biti obaviješten o restriktivnim mjerama u skladu sa Članom 3. nakon što se te mjere prestanu provoditi. Takvo obavještenje će biti odgođeno sve dok se ne bude mogla isključiti mogućnost da bi obavještavanje subjekta čiji se podaci čuvaju moglo ugroziti svrhu zbog koje su se podaci prikupljali, ili sve dok se mogu predvidjeti bilo kakve opće štete za interese Savezne države ili federalne jedinice. Prema odredbi 2, tamo gdje se to obavještenje odgodi dvanaest mjeseci nakon okončanja mjere, njegovo odgađanje zahtijeva odobrenje Komisije G10. Komisija G10 određuje trajanje daljnjeg odlaganja davanja obavještenja."[39]

"Kada se radi o prikupljanju podataka u skladu sa podčlanovima 2. i 1, čiji su priroda i značaj bitni za ograničenje privatnosti pisma, poštanske komunikacije i telekomunikacija, a posebno kada se radi o prisluškivanju i snimanju privatnih razgovora tajnim tehničkim sredstvima, tada će,

1. subjekt čuvanja podataka biti obaviješten o mjeri nakon njenog okončanja, čim se može odbaciti da je svrha mjere ugrožena, i
2. Parlamentarni kontrolni panel biti o tome obaviješten."[40]

3.3.6 Provjera, revizija i brisanje ličnih podataka

Drugi način na koji principi zaštite podataka mogu biti provedeni je nametanje dužnosti obavještajnim službama da periodično provjeravaju da li su njihovi dosjei sa ličnim podacima precizni, ažurirani i relevantni za njihov mandat.[41] U nekim zemljama ta dužnost je povezana sa dodatnim dužnostima ispravljanja ili uništavanja informacija koje su netačne[42] ili više nisu relevantne.[43]

Da bi njihovi izvještaji mogli biti zasnovani na preciznim informacijama, obavještajne službe treba da uspostave procedure radi provjere i revizije ličnih podataka kako bi osigurale da su ažurirani i potpuni (u mjeri u kojoj je to relevantno za zakonite aktivnosti službi). Zastarjele informacije mogu navesti na pogrešne zaključke i time biti opasnije čak i od neznanja. Nadalje, sa stanovišta subjekta podataka, manja je vjerovatnoća da će lična informacija koja je tačna i ažurirana za rezultat imati neku nepravdu, na primjer da ta osoba neće proći sigurnosnu provjeru ili da će dobiti negativnu odluku o imigraciji.

Okvir 8: Redovne procjene podataka koje čuvaju obavještajne službe: dobra praksa koju je identificirao specijalni izvjestilac UN-a

"Obavještajne službe provode redovne procjene relevantnosti i tačnosti ličnih podataka koje čuvaju. Od njih se zakonom zahtijeva da izbrišu ili ažuriraju svaku informaciju za koju se procijeni da je netačna ili da više nije relevantna za njihov mandat, rad nadzornih institucija ili moguće pravne postupke."[44]

Zbog preventivne i anticipatorne prirode procjene prijetnje od strane sigurnosnih i obavještajnih službi, neki pojedinci mogu legitimno postati predmet pažnje službi prije nego što se prikupe dodatne informacije kojima se utvrđuje da dalje prikupljanje podataka o njima nije potrebna. Za neku osobu se, na primjer, može ustanoviti da sarađuje sa osobom koja je legitimni predmet prikupljanja podataka, ali nije i njegov saučesnik. Ili, pak, subjekt provjere može jednostavno imati ime slično imenu subjekta legitimnog prikupljanja podataka. Zahtjev obavještajnoj službi da zatvori dosje o takvoj osobi može spriječiti moguću zloupotrebu.

Slično tome, neprovjerene i površne informacije o pojedincima prikupljene tokom operacije koja je već završena treba izbrisati. Njemački zakon koji utvrđuje aktivnosti Saveznog ureda za zaštitu Ustava sadrži nekoliko odredbi relevantnih za ovo pitanje. On utvrđuje, na primjer, da prikupljanje informacija mora prestati „čim je postignuta njena svrha ili ako postoje indikacije da se svrha uopće ne može postići, ili se ne može postići primjenom tih sredstava."[45] Zakon također nameće dužnost da se provjeravaju (svakih pet godina) prethodno prikupljeni podaci, isprave netačni podaci (sa netačnim ili osporenim podacima, označeni kao takvi u odnosnim dosjeima[46]), te da se izbrišu podaci koji više nisu potrebni (vidjeti Okvir 9). Pored toga što štite subjekte podataka, ove službe pomažu revizoru u obavljanju njegovog zadatka.

Okvir 9: Dužnosti da se pregledaju, isprave i izbrišu lični podaci prema zakonu u Njemačkoj

Ove odredbe njemačkog zakona ilustriraju principe provjere, revizije i brisanja:

"(1) Netačni lični podaci pohranjeni u dosjeima će biti ispravljeni od strane Saveznog ureda za zaštitu Ustava.

(2) Lični podaci pohranjeni u dosjeima će biti izbrisani od strane Saveznog ureda za zaštitu Ustava ako je njihovo pohranjivanje bilo nepotrebno, ili saznanje o njima nije više potrebno radi izvršavanja zadataka. Podaci neće biti izbrisani ako postoji razlog da se vjeruje da bi brisanje ugrozilo legitimne interese subjekta podataka. U tom slučaju podaci će biti blokirani i prenosit će se samo uz saglasnost subjekta podataka.

(3) Kada radi na posebnim slučajevima, Savezni ured za zaštitu Ustava će provjeriti u određenim periodima, nakon najmanje pet godina, da li se pohranjeni lični podaci moraju ispraviti ili izbrisati."[47]

4. ULOGA NADZORNIH TIJELA

Ovaj dio razmatra načine na koje nadzorna tijela mogu pratiti korištenje ličnih podataka od strane obavještajnih službi kako bi osigurali da ti podaci ne budu zloupotrijebljeni. Mada ovo poglavlje ima za fokus prvenstveno vanjski nadzor, značaj unutarnjih mehanizama ne

treba zanemariti. Oni uključuju specifične procedure za utvrđivanje kada dosjei trebaju biti otvoreni ili zatvoreni, koji službenici trebaju imati pristup tim dosjeima, kada njihov sadržaj treba biti pregledan, i kako će se čuvati na sigurnom.

Učinkovit vanjski nadzor, s druge strane, zavisi od postojanja nezavisnih tijela sa odgovarajućim zakonskim ovlastima i resursima da ostvare svoj mandat (vidjeti Tabelu 2). Specijalni izvjestilac UN-a je naglasio potrebu za nezavisnom institucijom koja „ima pristup svim dosjeima koje čuvaju obavještajne službe i ima ovlast da naredi otkrivanje informacija pojedincima, kao i uništenje dosjea ili ličnih informacija."[48] Povelja Evropske unije o temeljnim pravima naglašava potrebu da pridržavanje pravila o zaštiti podataka bude „podložno kontroli nezavisnog organa."[50] Na državnom nivou, Švedski zakon garantira autonomiju i resurse Švedskoj komisiji za sigurnost i zaštitu integriteta, dok mađarski zakon nameće specifičnu dužnost obavještajnim službama da sarađuju sa nezavisnim nadzornim tijelima u vezi sa korištenjem ličnih podataka od strane službi.[51]

TABELA 2: KARAKTERISTIKE VANJSKIH NADZORNIH TIJELA

Institucija	Nezavisnost	Djelokrug	Metode	Ishodi
Institucija ombudsmena	Autonomno	Pojedinačne žalbe	Istrage	Preporuka
Komesar za zaštitu podataka	Autonomno	Pridržavanje zakona o zaštiti podataka	Istrage, studije slučaja	Izvještaj, direktiva
Sud	Autonomno	Pojedinačne žalbe	Sudski proces	Obavezujuća odluka
Parlamentarni odbor	Partijsko	Upućivanja, izvještavanja na vlastitu inicijativu	Parlamentarna saslušanja	Izvještaj

U tranzicijskim i postkonfliktnim državama, nove demokratizirane službe često preuzimaju brigu o velikim arhivama dosjea sigurnosnih službi koji sadrže informacije prikupljene po nalogu prethodnog režima. Upravljanje tim dosjeima može donijeti neobične izazove, posebno kada je (iz razloga koje nalaže demokratija) sigurnosni i obavještajni sektor zemlje drastično smanjen. U tim situacijama nezavisna nadzorna tijela mogu igrati korisnu ulogu u reviziji prakse upravljanja dosjeima kroz primjenu različitih sredstava.

Općenito, funkcije nezavisnih nadzornih tijela u pogledu ličnih podataka dijelom se rukovode standardima utvrđenim zakonom o ljudskim pravima. Što se tiče naknadnih pravnih lijekova, na primjer, Član 13. ECHR zahtijeva da "Svako čija su prava i slobode … prekršeni ima djelotvoran pravni lijek pred državnim vlastima." Svojom odlukom u predmetu *Segerstedt-Wiberg protiv Švedske* (2006), ECtHR je utvrdio da, mada je test koji proizlazi iz Člana 13. generalno supsidijaran testovima iz Člana 8 „u skladu sa zakonom" i „potrebno u demokratskom društvu", odsustvo odredbe o pravnom lijeku u državnom zakonu može rezultirati kršenjem Konvencije. Na drugom mjestu je Sud utvrdio da, čak i u kontekstu državne sigurnosti, procedura pravnog lijeka koju zahtijeva Član 13. mora biti učinkovita u praksi kao i zasnovana na zakonu.[52]

U predmetu *Udruženje za evropske integracije i ljudska prava protiv Bugarske*, koji se tiče slučaja presretanja informacija u kojemu se navodi kršenje Člana 8. i Člana 13, Sud se sa

odobravanjem pozvao na nekoliko primjera nezavisnih pravnih lijekova koji zadovoljavaju zahtjeve Konvencije. Oni uključuju: pravo podnošenja žalbe stručnom nadzornom tijelu (Komisiji G10) i Ustavnom sudu u Njemačkoj, pravo podnošenja žalbe Državnom vijeću u Luksemburgu, pravo da se obrati Specijalnom tribunalu u Ujedinjenom Kraljevstvu, i pravo podnošenja žalbe stručnom nadzornom tijelu u Norveškoj.[53] (Za detaljnu raspravu o rješavanju žalbi, vidjeti Poglavlje 9 – Forcese).

Što se tiče korištenja ličnih podataka od strane obavještajnih službi, ključna pitanja nadzora odraz su pitanja koja se tiču pravnih standarda – prikupljanje podataka, pohranjivanje podataka, pristup podacima subjekta čiji se podaci čuvaju, obavještavanje, pregled, ispravljanje i brisanje. Stoga što je opseg ovih pitanja širok, nadležnost nadzornih tijela mora biti jednako široka. Ovlast njemačke Komisije G10, na primjer, obuhvata „cijeli spektar od prikupljanja, obrade do korištenja ličnih podataka pribavljenih u skladu sa ovim Zakonom od strane obavještajnih službi Federacije, uključujući odluku o obavještavanju subjekata podataka."[54]

Nadzor ove vrste potreban je kako bi se osiguralo da se službe pridržavaju standarda o ličnim podacima koji su gore razmatrani. S obzirom na tajnovitu prirodu obavještajnog rada, takav nadzor će vjerovatnije biti učinkovit i nailaziti na poštovanje javnosti ako je kontinuiran (ili barem periodičan), a ne jednostavno reakcija na žalbe javnosti ili navode o zloupotrebi. Jedan broj zemalja, stoga, osigurao je tekuću kontrolu kroz mandat nezavisnih tijela odgovornih za nadzor nad obavještajnim službama. U Norveškoj, na primjer, Parlamentarni odbor za nadzor nad obavještajnim službama (stručno nadzorno tijelo) ima zakonsku dužnost da provodi šest inspekcija Norveške policijske sigurnosne službe godišnje. Te inspekcije moraju uključiti barem deset nasumičnih provjera arhiva i barem dva puta godišnje pregled svih tekućih predmeta tajnog praćenja.[55] Danski kontrolni odbor za policijsku i vojnu obavještajnu službu (Wambergov odbor) koji je nazvan po njegovom posljednjem predsjedavajućem, A. M. Wambergu – ima sličnu ulogu (vidjeti Okvir 10).

Okvir 10: Danski Odbor za kontrolu policijske i vojne obavještajne službe (Wambergov odbor)

Primarni zadatak Wambergovog odbora je nadzor nad registracijom i diseminacijom ličnih podataka od strane Danske sigurnosne i obavještajne agencije (PET). Kada neka osoba ili organizacija postanu predmet obavještajne istrage, PET može tražiti da registrira dosjee o toj osobi ili organizaciji. Ti dosjei su predmet provjere od strane Wambergovog odbora, koji mora odobriti registraciju novih dosjea o Dancima i stranim državljanima koji borave u Danskoj.

Odbor čine predsjedavajući i još tri člana. Svi su imenovani na temelju općeg povjerenja i poštovanja koje uživaju. Svakog od njih javnost mora također percipirati kao apolitičnog.

Odbor se sastaje šest do deset puta godišnje u uredima PET-a kako bi razmotrio predmete i odlučio da li su ispunjeni kriteriji za njihovu registraciju. U isto vrijeme, Odbor nasumice uzima uzorke starih dosjea kako bi utvrdio da li su rokovi za njihovo brisanje ispunjeni. Odbor također redovno sa Ministarstvom pravde raspravlja o principima registracije.

U jednom broju zemalja, pojedinac koji se žali na način kako je obavještajna služba upravljala njegovim ili njenim ličnim podacima može biti saslušan od nezavisnog tijela koje ima ovlast da provodi inspekciju dosjea službe i utvrđuje da li su ti podaci zloupotrijebljeni (vidjeti Forcese –Poglavlje 9). Po švedskom zakonu, na primjer, Komisija za sigurnost i

zaštitu integriteta ima ovlast, kada postupa po žalbi, da provjeri zakonitost aktivnosti sigurnosne službe vezanih za korištenje ličnih podataka (vidjeti Okvir 11). Komisija također ima ovlast da provjeri objavljivanje ličnih podataka koji se čuvaju u raznim policijskim i sigurnosnim registrima kako bi se osiguralo da to bude u skladu sa švedskim zakonima i Ustavom, uključujući standarde ljudskih prava i princip srazmjernosti.[56]

Okvir 11: Švedska Komisija za sigurnost i zaštitu integriteta

Ove odredbe Švedskog zakona opisuju odgovornosti Komisije za sigurnost i zaštitu integriteta (stručno nadzorno tijelo):

"1. Komisija za sigurnost i zaštitu integriteta (Komisija) će nadzirati korištenje, od strane agencija za borbu protiv kriminala, metoda tajnog nadzora i lažnih identiteta i uz to vezane aktivnosti.

Komisija će također nadzirati obradu podataka od strane Švedske sigurnosne službe u skladu sa Zakonom o policijskoj zaštiti podataka, posebno u pogledu Člana 5. ovog Zakona.

Nadzor ima za cilj posebno osiguranje da aktivnosti navedene u prvom i drugom stavu se provode u skladu sa zakonom i drugim propisima.

2.Komisija će vršiti nadzor putem inspekcija i drugih istraga.

Komisija može dati izjave o utvrđenim okolnostima i izraziti svoje mišljenje o potrebi za promjenama u aktivnostima, te će nastojati da osigura da bilo kakvi nedostaci u zakonima i drugim propisima budu ispravljeni.

3. Na zahtjev pojedinca, Komisija je obavezna provjeriti da li je on ili ona bio predmet tajnog praćenja ili predmet obrade ličnih podataka kako je to definirano u Članu 1, te da li je korištenje tajnog praćenja i uz to vezane aktivnosti ili obrada ličnih podataka bilo u skladu sa zakonima i drugim propisima. Komisija će obavijestiti tog pojedinca da je provjera bila izvršena."[57]

5. PREPORUKE

Ovo poglavlje preporučuje principe koje osobito parlamentarci mogu slijediti u uspostavi odgovarajućeg zakonskog okvira za korištenje ličnih podataka od strane obavještajnih službi na način koji je u skladu sa obavezama vezanim za ljudska prava.

- Zakon koji propisuje mandat svake obavještajne službe treba sadržavati svrhe u koje se lični podaci mogu zakonito prikupljati i dosjei zakonito otvarati.
- Zakon kojim se uređuje rad obavještajnih službi treba da uspostavi učinkovite kontrole korištenja ličnih podataka i koliko dugo se podaci mogu sačuvati. Te kontrole treba da budu u skladu sa međunarodno prihvaćenim principima zaštite podataka. Zakon treba također da zahtijeva provjere koje će obavljati nezavisni službenici (to jest, ljudi zaduženi za nadzor, ali koji su izvan obavještajne zajednice), kako bi se osiguralo da kontrole budu zaista učinkovite.
- Zakon o obavještajnim službama ne smije izuzimati obavještajne službe iz domaćih zakona o privatnosti i zaštiti ličnih podataka. Umjesto toga, službama treba dozvoliti, kada je to relevantno za njihov mandat, da koriste mogućnost nametanja izuzetaka u odnosu na propise o otkrivanju informacija na osnovu ograničenog koncepta državne sigurnosti.

- Zadatak utvrđivanja da li su takvi izuzeci primijenjeni ispravno je na nezavisnom nadzornom tijelu koje ima odgovarajući pristup relevantnim podacima u dosjeima službe.
- Pojedinci koji se žale da je pohranjivanje, korištenje ili otkrivanje njihovih ličnih podataka od strane obavještajne službe predstavljalo kršenje njihove privatnosti treba da imaju pravo na učinkovit pravni lijek pred nezavisnim tijelom.
- Odluke obavještajnih službi o pohranjivanju ličnih podataka treba provjeravati nezavisno nadzorno tijelo, jednako kao i zahtjeve subjekata čiji se podaci čuvaju i odluke da se čuvaju, prenose ili brišu lični podaci.

Bilješke

1. Ova definicija pojavljuje se u Čl. 2(a) Konvencije Vijeća Evrope o zaštiti pojedinaca u pogledu automatske obrade ličnih podataka Vijeća Evrope i Čl. 1(b) Smjernica Organizacije za ekonomsku saradnju i razvoj (OECD) o zaštiti privatnosti i prekograničnim tokovima ličnih podataka. Slična definicija pojavljuje se u Čl. 2(a) Direktive Evropske unije 95/46/EC. Međutim, ova direktiva ne primjenjuje se na aktivnosti državne sigurnosti (vidjeti Čl. 3.2).
2. Čl. 17. Međunarodnog pakta o građanskim i političkim pravima navodi da: "1. Niko ne može biti izložen proizvoljnom ili nezakonitom miješanju u privatni život, porodicu, stan ili prepisku, niti protivzakonitim napadima na čast i ugled. 2. Svako ima pravo na zakonsku zaštitu od takvog miješanja ili napada." Čl. 12. Opće deklaracije o ljudskim pravima navodi da "Niko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, porodicu, dom ili prepisku, niti napadima na njegovu čast i ugled. Svako ima pravo na pravnu zaštitu protiv takvog miješanja ili napada."
3. *Leander protiv Švedske*, br. 9248/81, Evropski sud za ljudska prava (ECHR), 1987.
4. *Rotaru protiv Rumunije*, br. 28341/95, ECHR, 2000, pasus 46.
5. *Weber i Saravia protiv Njemačke*, br. 54934/00, ECHR, 2006, pasus 84.
6. *R. V. v. The Netherlands*, br. 14084/88, ECHR, 1991.
7. *Weber and Saravia v. Germany*, br. 54934/00, ECHR, 2006, pasus 93.
8. Ibid., pasus 94.
9. Vidjeti, na primjer, detaljnu analizu njemačkog Zakona o G10 u predmetu *Weber i Saravia protiv Njemačke*, odluka o prihvatljivosti, br. 54934/00, ECHR,2006.
10. *Shimovolos v. Russia*, br. 30194/09, ECHR,2011.
11. *Leander v. Sweden*, br. 9248/81, ECHR, 1987.
12. *Rotaru v. Romania*, br. 28341/95, ECHR, 2000.
13. Ibid., pasus 57.
14. Ibid.
15. *Segerstedt-Wiberg and Others v. Sweden*, br. 62332/00, ECHR, 2006.
16. *Leander v. Sweden*, br. 9248/81, ECHR, 1987, Paragraphs 52¬–57; see also *Rotaru v. Romania*, br. 28341/95, ECHR, 2000, pasus 59.
17. *Turek v. Slovakia*, br. 57986/00, ECHR, 2006.
18. *Haralambie v. Romania*, br. 21737/03, ECHR, 2009.
19. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010),str. 21 (Practice 23).
20. Vijeće Evrope, Konvencija o zaštiti pojedinaca u pogledu automatske obrade ličnih podataka, ETS br. 108 (Strasbourg, 28.I.1981). Konvencija se naslanja na veoma utjecajne Smjernice o zaštiti privatnosti i prekograničnih tokova ličnih podataka (23. septembar 1980.) (dostupno na http://www.oecd.org/document/18/0,3 343,en_2649_34255_1815186_1_1_1_1,00. html#part2).Smjernice OECD-a uspostavljaju osam osnovnih principa zaštite podataka vezano za ograničenje u prikupljanju, kvalitet podataka, specifikaciju svrhe, ograničenje korištenja, sigurnosne garancije, otvorenost, pojedinačno učešće, i odgovornost.
21. Ibid., Čl. 4.
22. Ibid., Čl. 10.
23. Termin *potrebna mjera* treba razumjeti u kontekstu doktrine proporcionalnosti kako je ona formulirana u Povelji o temeljnim pravima Evropske unije.
24. Vijeće Evrope, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS br. 108 (Strasbourg, 28.I.1981), Čl. 9.
25. Germany, Federal Act on Protection of the Constitution (20 December 1990), *Federal Law Gazette I*, str. 2954, 2970, posljednji put dopunjen Čl. 1.a Akta od 31. jula 2009, *Federal Law Gazette I*, str. 2499, 2502, Čl. 9.
26. Holandija, Intelligence and Security Services Act 2002, Čl. 13.
27. Argentina, National Intelligence Law 2001, br. 25520, Čl. 4.
28. Law on the National Security of Romania, Čl. 21.
29. Kanada, Privacy Act, R.S.C., 1985, Poglavlje P-21, Čl. 10. Pregled banaka podataka ličnih informacija koje čuvaju sigurnosne i obavještajne službe Kanade mogu se naći na http://www.infosource.gc.ca/inst/csi/fed07-eng.asp. dead link
30. Holandija, Intelligence and Security Services Act 2002.
31. Npr. vidjeti Holandija, Intelligence and Security Services Act 2002, Čl. 47; Švedska, Act on Supervision of Certain Crime-Fighting Activities, Čl. 3; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, Čl. 18 (1).
32. Vidjeti, npr, Holandija, Intelligence and Security Services Act, Čl. 53–56; Hrvatska, Zakon o

sigurnosno-obavještajnom sustavu, Čl. 40 (2) (3).

33. Ian Leigh, "Legal Access to Security Files: the Canadian Experience," *Intelligence and National Security* Vol. 12, br. 2 (1997), str. 126. Za potrebe ove studije obavljeni su razgovori sa službenicima Kanadske sigurnosno-obavještajne službe, komesari za informacije i privatnost i njihovim službenicima, te onima na koje se zakon primjenjuje, sudijama saveznog suda, i drugim stručnjacima.
34. Ujedinjeno Kraljevtsvo, Data Protection Act 1998, Čl. 28.
35. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010), str. 23 (praksa 26).
36. Prema Čl. 34. Zakona o obavještajnim i sugurnosnim službama iz 2002, počevši pet godina nakon što je obavještajna služba iskoristila posebnu istražnu ovlast (i nakon toga svake godine), "nadležni ministar će razmotriti da li se izvještaj o događaju može dostaviti osobi u vezi sa kojom je jedna od tih posebnih ovlasti korištena. Ako je to moguće, onda će se desiti što je prije moguće."
37. Njemačka, Federal Act on Protection of the Constitution,Čl. 9.3.
38. Holandija, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2010–2011*, Poglavlje 4.
39. Njemačka, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (Juni 26, 2001), *Federal Law Gazette I*, str.. 1254, revidiran 2298, posljednji put dopunjen Čl. 1. Akta od 31. jula 2009, *Federal Law Gazette I*, str. 2499, Čl. 12.1.
40. Njemačka, Federal Act on Protection of the Constitution, Čl. 9.3.
41. Npr. Njemačka, Federal Act on Protection of the Constitution, Section 14.2; Njemačka, G10 Act, Čl. 4.1 i 5; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure,Čl. 15 (1) (5).
42. Holandija, Intelligence and Security Services Act, Čl. 43; Hrvatska, Zakon o sigurnosno-obavještajnom sustavu, Čl. 41(1).
43. Njemačka, Federal Act on Protection of the Constitution, Čl. 12.2.
44. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010), str. 22 (Praksa 24).
45. Njemačka, Federal Act on Protection of the Constitution, Čl. 9.1.
46. Ibid., Čl. 13.
47. Ibid., Čl. 12.
48. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010), str. 22 (Praksa 25).
49. Evropska unija, Charter of Fundamental Rights of the European Union, Čl. 8.3.
50. Švedska, Ukaz sa uputama za Švedsku komisiju za sigurnost i zaštitu integriteta, Čl. 4–8 (o managementu i odlučivanju) i 12¬–13 (o resursima i podršci).
51. Mađarska, Act on the National Security Services, Čl. 52.
52. *Al-Nashif v. Bulgaria*, br. 50963/99, ECHR, 2002, Pasus 136.
53. *Association for European Integration and Human Rights v. Bulgaria*, br. 62540/00, ECHR, Pasus 100.
54. Hans De With and Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies u Njemačkoj," u *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (br.ussels: European Parliament, 2011), Annex A, str. 220.
55. Norveška, Instructions for Monitoring of Intelligence, Surveillance and Security Services, Čl. 11.1 (c) i 11.2 (d).
56. Iain Cameron, "Parliamentary and Specialised Oversight of Security and Intelligence Activities in Sweden," u *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (br.ussels: European Parliament, 2011), str. 279–81.
57. Švedska, Act on Supervision of Certain Crime-Fighting Activities (2007); vidjeti također Švedska,

Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection (2007) Čl. 2 (dostupno na http://www.sakint.se/dokument/english/ordinance_instruction_scsip.pdf).

POGLAVLJE 7

Nadzor nad razmjenom informacija

Kent Roach

SEDAM

7

Nadzor nad razmjenom informacija

Kent Roach

1. UVOD

Ovo poglavlje propituje izazove što za nadzor nad obavještajnim službama i drugim državnim organima koje sakupljaju, analiziraju i distribuiraju državne sigurnosne informacije, predstavlja povećana razmjena informacija.[1] Termin *razmjena informacija* ovdje se odnosi na informacije koje se razmjenjuju među obavještajnim službama i partnerskim agencijama, bilo da su strane ili domaće. Mada je fokus ovog poglavlja načelno na nadzornim tijelima, ona razmatra i posljedice sve veće razmjene informacija za ljudska prava i privatnost – što može biti od interesa za druga tijela, npr. za sudsku i izvršnu granu vlasti, medije i civilno društvo.

Obavještajne službe oduvijek su imale zadatak da razmjenjuju informacije koje prikupljaju. Od terorističkih napada koji su se desili 11. septembra 2001. godine, međutim, mnogo veći naglasak se stavlja na razmjenu informacija između obavještajnih službi i drugih tijela na međunarodnom nivou. Iz očiglednih razloga, porast količine razmijenjenih informacija i broj službi koje su u to uključene doveo je do porasta broja problema vezanih za razmjenu informacija. Informacija koja je razmijenjena može biti netačna, što kao rezultat ima pogrešno usmjeravanje ionako nedovoljnih resursa primaoca. Usto, služba koja dobije informacije može ih koristiti u pogrešne svrhe. U nekim krajnjim slučajevima, to može čak dovesti do toga da služba postane saučesnik u mučenju i drugim kršenjima ljudskih prava koja čine isporučilac ili primalac informacije.

Loše prakse u razmjeni informacija mogu ozbiljno štetiti ugledu zemlje koja ih pruža, kao što su pokazala nedavna otkrića o razmjeni informacija između obavještajnih službi Libije, Amerike i Velike Britanije.[2] Čak i teže štetne efekte može na ugled pojedinca imati pogrešna razmijenjena informacija. Te žalosne posljedice čine posebno važnim činjenicu da prakse razmjene informacija treba podvrgnuti učinkovitom nadzoru, mada su informacije koje se razmjenjuju često veoma strogo klasificirane. Nadzor nad praksom razmjene informacija posebno je važan s obzirom na to da se ove aktivnosti obično provode u tajnosti te ih, stoga, nije lako provjeravati u sudovima ili medijima. Oni koji mogu biti negativno pogođeni razmijenjenim informacijama možda čak i ne znaju za to i možda neće biti u prilici da podnesu žalbu. Općenito govoreći, nadzorna tijela treba da imaju pristup razmijenjenim informacijama jer, inače, neće biti u stanju učinkovito provjeravati prakse razmjene informacija obavještajnih službi koje nadziru. Međutim, nedavno intenziviranje razmjene informacija, kao i tajnost razmijenjenih informacija, predstavlja izazove za nadzorna tijela koji se nikako ne mogu podcijeniti.

Ovo poglavlje počinje kratkim razmatranjem razmjene informacija u svijetu nakon 11. septembra. Glavni dio teksta razmatra izazove koje predstavlja nadzor nad vanjskom, a potom unutrašnjom, razmjenom informacija kako u pogledu prijema, tako i u pogledu diseminacije informacija. Ovo poglavlje u zaključku daje konkretne preporuke za poboljšanje nadzora nad razmjenom informacija. Preporuke se tiču ne samo političkog, organizacijskog i upravljačkog aspekta nadzora, već i pravnog okvira u kojem se razmjenom informacija može učinkovitije upravljati.

2. RAZMJENA INFORMACIJA

2.1 POTREBA ZA RAZMJENOM INFORMACIJA

Očito je da i strane i domaće obavještajne službe treba da razmjenjuju informacije ukoliko se žele učinkovito baviti složenim sigurnosnim prijetnjama s kojima su suočene. U sadašnjem transnacionalnom okruženju, međutim, često se naglašava potreba za još većom razmjenom informacija. Na primjer, u Rezoluciji 1373 (28. septembar 2001), Vijeće sigurnosti Ujedinjenih nacija jasno je pozvalo na intenziviranje razmjene informacija među državama članicama. U Evropi, institucije poput Europol-a, Bernskog kluba i Vojnog osoblja Evropske unije, te Situacijskog centra Evropske unije, također zahtijevaju sve veću razmjenu informacija.[3] Kao rezultat, zemlje sa vrlo različitim tradicijama, koje inače mogu biti nevoljne za učešće u zajedničkim sigurnosnim operacijama, sada su ipak spremne da razmjenjuju informacije koje se tiču ne samo borbe protiv terorizma, već i vojnih i mirovnih operacija, inspekcija oružja i krivičnih gonjenja počinilaca ratnih zločina.

Mjeru u kojoj se razmjena informacija danas odvija među obavještajnim službama teško je ustanoviti zato što su te informacije tajne, te su time i metode i aranžmani kojima se one dijele tajna. Podaci kojima raspolažemo, međutim, daju nam određenu predstavu o kojoj količini se radi. Domaće obavještajne službe Kanade i Australije, na primjer, razmjenjuju informacije sa oko 250 stranih agencija. Američka centralna obavještajna agencija (CIA) povezana je sa preko 400 agencija širom svijeta.[4] Ova razmjena se odvija i formalno i neformalno.

Zbog složene prirode današnjeg okruženja kad su u pitanju sigurnosne prijetnje, zemlje

koje poštuju ljudska prava mogu povremeno osjećati pritisak da moraju razmjenjivati informacije i sa državama koje ne poštuju dovoljno ljudska prava. Određena služba može smatrati da mora upozoriti zemlju na osumnjičenog teroristu koji je ušao ili planira ući u neku drugu zemlju, čak i ako je zemlja koja dobiva tu informaciju možda već registrirana kao zemlja u kojoj se krše ljudska prava. Također je činjenica da oni koji pružaju informacije razumljivo očekuju visok stepen reciprociteta od primalaca informacija.

U deceniji nakon 11. septembra, vlade mnogih država radile su na otklanjanju pravnih i organizacijskih prepreka za razmjenu informacija između svojih agencija zaduženih za sigurnost i obavještajni rad. To se posebno odnosi na Sjedinjene Države, gdje je jedna vladina komisija utvrdila da su prepreke koje su postojale između obavještajnih i sigurnosnih agencija možda spriječile identifikaciju nekih od osoba koje su 11. septembra otele avione.[5] Rezultat te spoznaje je povećana spremnost na razmjenu informacija koja se ne odnosi samo na borbu protiv terorizma, već na široki spektar odgovornosti vezanih za provedbu zakona koji uključuje sigurnost granica, imigraciju, krijumčarenje i špijunažu.

2.2 PROBLEMI KOJE IZAZIVA RAZMJENA INFORMACIJA

Mada postoji opća saglasnost da je razmjena informacija potrebna radi veće sigurnosti, nedavna ekspanzija razmjene informacija dovela je do izvjesnog broja potencijalnih problema koji traže budno upravljanje i nadzor. Na primjer, agencije za provedbu zakona sada će vjerovatnije preduzeti akcije na osnovu razmijenjenih informacija koje su nepouzdane, a postoji i veći rizik da će informacije koje razmijene obavještajne službe biti otkrivene u postupcima pred sudovima. Pojedinci su također izloženi većem riziku da će njihova prava, pogotovo pravo na privatnost, biti prekršena. Usto, pojedinci rijetko imaju priliku da ospore tačnost razmijenjenih informacija zato što često nisu ni svjesni da su informacije o njima razmijenjene i neće imati pristup razmijenjenim informacijama.

U mnogim zemljama, obavještajne službe tradicionalno su nespremne razmjenjivati tajne informacije sa policijom i drugim agencijama za provedbu zakona. Jedna istražna komisija u Kanadi zaključila je da je ta nespremnost doprinijela uspjehu operacije postavljanja bombe u avion Air India 1985. godine, kao i raznim drugim manjkavostima tokom istrage nakon samog događaja.[6] Obavještajne službe imaju tendenciju da čuvaju informacije zato što se boje da će njihova razmjena u konačnici rezultirati njihovim otkrivanjem, što može važne izvore i metode izložiti riziku te time ugroziti sposobnost službe da prikuplja obavještajne informacije u budućnosti. Nadalje, ako je informacija dobivena na način koji je čini neprihvatljivom u sudskom postupku, njena razmjena sa agencijama za provedbu zakona može biti još problematičnija. Policijske snage, mada su možda čak spremnije od obavještajnih službi da razmjenjuju informacije, također brine to da će razmjena informacija umanjiti njihovu sposobnost da istražuju i krivično gone slučajeve sigurnosnih prijetnji.

Tijela zadužena za nadzor nad obavještajnim i sigurnosnim službama suočena su sa nekim od najvećih izazova. Moraju se nositi sa ogromnom količinom informacija koje razmjenjuju, čiji obim je toliki da su redovno prisiljeni oslanjati se na to da ocjenjuju samo određenu količinu informacija. Većina nadzornih tijela se suočava i sa teškoćama u pristupu i praćenju traga tajnih informacija koje se razmjenjuju. Na primjer, nadzorno tijelo za policiju možda nema ovlast da utvrđuje na koji je način prikupljena informacija koju je policija dobila od obavještajne službe. To posebno važi za situaciju kada je pružalac informacije neka strana agencija.

U mnogim državama, uspostavljene su mreže obavještajnih i sigurnosnih službi (koje se nekada zovu i „centri za fuziju“) kako bi se na jednom mjestu sabirale informacije o sigurnosnim prijetnjama koje se dobijaju iz domaćih i stranih izvora. Neke od tih mreža čak omogućavaju stranim agencijama da međusobno razmjenjuju informacije. Domaća nadzorna tijela trebaju imati pristup informacijama koje su prikupljene i distribuirane kroz te mreže, ako žele u potpunosti razumjeti operacije agencije za čiji su nadzor zadužena – posebno pošto agencija daje i dobiva informacije od tih regionalnih, državnih i supradržavnih institucija.

Jedan odgovor na povećanu razmjenu informacija, kako između domaćih, tako i sa stranim agencijama je pokretanje ad hoc istraga sa specijalnim zadatkom razmatranja razmjene informacija između više agencija. Sljedeća dva okvira razmatraju primjere takvih *ad hoc* istraga u Kanadi i Ujedinjenom Kraljevstvu.

Obavještajne i sigurnosne službe imaju očitu potrebu da razmjenjuju informacije sa domaćim i stranim partnerima. Agencija koja isključivo prikuplja informacije, a ne razmjenjuje ih, neće uspjeti obaviti svoju dužnost da upozorava druge na sigurnosne prijetnje koje otkrije. Transnacionalna priroda mnogih današnjih prijetnji ukazuju na nužnost povećanja razmjene informacija - kako u zemlji, tako i u svijetu.

Povećana razmjena informacija, međutim, nije bez nedostataka. Ona može dovesti do kršenja prava na privatnost i drugih ljudskih prava na načine koji nisu ni zakonski odobreni, niti su etički opravdani. Ona također krije rizik otkrivanja tajnih informacija dobivenih iz osjetljivih izvora.

Razmjena informacija putem domaćih i naddržavnih mreža (centri za fuziju) može umanjiti i ugroziti odgovornost. Zakonodavna i stručna nadzorna tijela, čiji mandat ograničava njihove nadležnosti na jednu agenciju, često nemaju pristup evidencijama mreža u kojima obavještajne i sigurnosne službe učestvuju, a nedostatak pristupa može ozbiljno onemogućiti njihov rad na nadzoru.

Razmjena informacija preko državnih granica može također izazvati sukob u smislu politika, kao što su situacije kada se zemlje sa dobrim rezultatima u pogledu zaštite ljudskih prava nađu u situaciji da razmjenjuju informacije sa zemljama koje imaju loše rezultate u pogledu zaštite ljudskih prava. Razmjena informacija na taj način može jednu državu učiniti saučesnikom u kršenju ljudskih prava, kao što je mučenje koje provodi njen partner u razmjeni informacija.

Ukratko, obavještajne i sigurnosne službe neće obavljati dobro svoj posao ako potpuno odbiju razmjenu informacija. S druge strane, povećana razmjena informacija krije u sebi brojne rizike. Rizici za pojedince uključuju kršenje ljudskih prava, posebno prava na privatnost. Rizici za obavještajne i sigurnosne službe uključuju diseminaciju nepouzdanih i/ili nepropisno pribavljenih informacija koje mogu štetiti ugledu službe i rezultirati pogrešnom raspodjelom ionako nedovoljnih sredstava. Rizici za nadzorna tijela uključuju nova ograničenja njihove sposobnosti da ustanove koje se informacije razmjenjuju i na koji način se odvija ta razmjena.

Okvir 1: Kanadske *ad hoc* istrage o razmjeni informacija

Prema izvještajima dvije kanadske istražne komisije koje su osnovane na višegodišnji mandat (Istražna komisija o djelovanju kanadskih službenika u vezi sa slučajem Mahera Arara i Interna istraga o djelovanju kanadskih službenika u vezi sa Abdullahom Almalkijem, Ahmadom Abou-Elmaatijem i Muayyedom Nureddinom), prakse razmjene informacija koje primjenjuju kanadska policija i obavještajne službe direktno su doprinijele mučenju kanadskih građana koji su bili pritvoreni u Siriji i Egiptu pod sumnjom terorizma.[7] Obje komisije su bile *ad hoc* tijela imenovana od vlade prvenstveno kao reakcija na javni skandal, ali i zbog sve veće svijesti o činjenici da postojeće nadzorne institucije, već opterećene obavezom da nadziru određene agencije, nisu imale nadležnosti da razmotre kako je vlada u cjelini odgovorila na široka međunarodna sigurnosna pitanja.

Obje komisije pozvale su Američku, Egipatsku i Sirijsku vladu da sarađuju u njihovoj istrazi. Sve tri strane vlade, međutim, to nisu učinile. Usto, kanadska vlada je nametnula ograničenja na mogućnost da komisije objave tajne informacije do kojih su došle. Međutim, pošto su ta ograničenja bila predmet sudske ocjene, komisije su uspjele u nekim slučajevima otkriti više informacija nego što je to vlada isprva željela – bilo kroz uspješan sudski postupak ili mogućnost da će se takav postupak održati.

Komisije su donekle razmotrile informacije koje je Kanada razmijenila sa zvaničnicima SAD-a, Sirije i Egipta. Te su informacije uključivale obavještajne informacije koje razne Kanađane povezuju sa terorističkim grupama. Konkretnije, sadržavale su i listu pitanja koja su kanadski zvaničnici poslali sirijskim i egipatskim zvaničnicima da se, prilikom ispitivanja, postave kanadskim građanima pritvorenim u Siriji i Egiptu osumnjičenim za terorizma.

Kanadske komisije su također provjerile informacije dobivene od tih stranih zvaničnika, koje su kasnije bile distribuirane unutar Kanade i uvedene kao dokazna građa u barem jedan sudski postupak. Obje komisije su pronašle nedostatke u načinu kako su te informacije razmijenjene – ne samo među domaćim policijskim, sigurnosnim, carinskim i diplomatskim službenicima, već i sa stranim agencijama.

Ove dvije istrage usmjerile su se prvenstveno na ispravnost postupka razmjene informacija, posebno opasnost koju one predstavljaju za ljudska prava, kao što je pravo da osoba ne bude podvrgnuta mučenju i pravo na privatnost. Ipak, bilo bi netočno reći da su komisije bile protiv povećane razmjene informacija. One su prosto željele bolju kontrolu i jače provjere. Komisija u slučaju Arar zaključila je da je „razmjena informacija od vitalnog značaja, ali se mora vršiti na pouzdan i odgovoran način. Potreba za razmjenom informacija ne znači da se informacije moraju razmjenjivati bez kontrole, pogotovo bez korištenja upozorenja. To također ne znači ni da se informacije mogu razmjenjivati a da se ne obraća pažnja na njihovu relevantnost, pouzdanost ili tačnost, ili na zakone koji štite lične informacije ili ljudska prava."[8]

Treća kanadska istraga u kojoj je razmatran slučaj bombe postavljene u avion aviokompanije Air India 1985. godine, bavila se je razmjenom informacija iz donekle drugačije perspektive, istražujući efikasnost razmjene informacija (nasuprot njenoj ispravnosti). Komisija je tom prilikom razradila preporuke koje su osmišljene tako da pruže pravni lijek u slučaju nespremnosti obavještajnih službi da razmjenjuju informacije sa policijom i drugim agencijama za provedbu zakona iz bojazni otkrivanja tajni.

Sve tri komisije su ukazale na temeljnu dilemu razmjene informacija: premalo razmjene prijeti sigurnosti; previše razmjene, posebno kada se razmjena vrši na nedisciplinirani način, predstavlja prijetnju za ljudska prava.

Okvir 2: Britanska *ad hoc* istraga o razmjeni informacija

Britanska vlada je 2010. godine pokrenula službenu istragu (istraga o pritvorenicima) o tome koliko su Britanci sudjelovali u mučenju pritvorenika koje su u pritvoru držale druge zemlje.

Na početku je pripremljen protokol u kojem je navedeno da će Vlada pružiti istražnom timu sve relevantne informacije, osim ako je pružanje tih informacija u sukobu sa postojećim obavezama koje se tiču povjerljivosti.[9] U Protokolu je također navedeno da će sekretar ministarstva u krajnjoj instanci odlučivati koji materijal može biti objavljen. Svrha ove odredbe je bila da se osigura da ne bude učinjena šteta po javni interes kroz neovlašteno otkrivanje informacija vezanih za državnu sigurnost, međunarodne odnose, odbranu i privredu. Taj proces znatno se razlikuje od procesa koji su koristile tri kanadska istražna tima, koji je razmatran ranije u ovom dijelu, zato što u britanskom slučaju nije postojala nijedna odredba koja bi omogućila sudsku reviziju odluka Vlade da ne otkrije tajne informacije. U svjetlu tih i drugih ograničenja, nekoliko organizacija za ljudska prava odbilo je učestvovati u istrazi.

U januaru 2012. godine, Vlada Ujedinjenog Kraljevstva prekinula je istragu uslijed stalnih odlaganja izazvanih potrebom da se sačeka okončanje krivičnih istraga – nekih aktivnosti koje je istraga trebalo da ispita – prije nego što bi istraga uopće mogla započeti. Iako je ova široka *ad hoc* istraga mogla potencijalno biti izuzetan primjer nadzora, oslanjanje britanske vlade na diskrecione i prijelazne mjere naglašava ograničenja stalnih nadzornih struktura te zemlje.

3. NADZOR NAD RAZMJENOM INFORMACIJA SA STRANIM AGENCIJAMA

Razmjena informacija sa stranim agencijama općenito nosi najveće izazove za nadzorna tijela i najveće rizike za ljudska prava. Strane agencije mogu uključivati obavještajne službe, policijske službe i druge grane stranih vlada sa pristupom diplomatskim kanalima komunikacije. One također mogu uključivati naddržavne mreže u kojima učestvuje jedna ili više tih agencija. Jedan komentator je zapazio da, nasuprot domaćoj razmjeni informacija, koja može biti podložna centraliziranoj kontroli, „u haotičnom međunarodnom svijetu... ne pridržavaju se sve zemlje normi privatnosti i drugih temeljnih sloboda. Pravo na privatnost je, stoga, ostavljeno na milost i nemilost svakoj pojedinačnoj obavještajnoj agenciji u mreži."[10]

Ostala prava koja su izložena riziku uključuju pravo da se ne bude podvrgnuto mučenju ili drugim oblicima surovog, neuobičajenog ili ponižavajućeg postupanja. Kako je zapazila Komisija za slučaj Arar u Kanadi, „razmjena informacija iz istraga u Kanadi sa drugim zemljama može imati 'domino efekt' koji prelazi kanadske granice, sa posljedicama koje će možda biti nemoguće kontrolirati iz same Kanade."[11] U najgorem slučaju, informacije poslane nekoj stranoj agenciji ta agencija može koristiti kao opravdanje za pritvor bez sudskog naloga, mučenje i čak ubistva. Nasuprot tome, informacija dobivena od strane agencije možda je dobivena mučenjem ili može biti kompromitirana na neki drugi način.

Iz očitih razloga, obavještajne i policijske službe su općenito loše obaviještene o izvorima i metodama koje su strane agencije koristile za dobivanje informacija. To predstavlja problem, zato što korišteni izvori i metode utječu kako na pouzdanost informacija, tako i na obavezu primaoca da poštuje ljudska prava. Slično tome, pružaoci informacija su

često slabo obaviješteni o tome kako će strana agencija koristiti dostavljene informacije. Agencije koje daju informacije nekad uz njih prilože upozorenja kojima se ograničava korištenje razmijenjenih informacija, ali pružaoci nemaju načina da osiguraju da strani partneri poštuju ta ograničenja. Međunarodna razmjena informacija ponekad je podređena suverenitetu države i potrebi da se zaštiti tajnost izvora, kao i metoda i korištenja obavještajnih informacija. Domaća nadzorna tijela mogu imati nadležnosti nad agencijama koje šalju ili onima koje dobivaju informacije, ali ne nad objema kad je jedna od tih agencija strana. Tako, u praksi, prilikom razmjene informacija, ona mogu nadzirati samo jednu stranu razmjene.

3.1 LOŠE PRAKSE U MEĐUNARODNOJ RAZMJENI INFORMACIJA

U posljednje vrijeme, najzloglasniji primjer loše prakse u međunarodnoj razmjeni informacija bio je slučaj Mahera Arara. Nakon napada 11. septembra, operativci Kraljevske kanadske konjičke policije razmijenili su sadržaj jedne istražne baze podataka sa zvaničnicima Vlade SAD-a. Nijedna od informacija nije bila unaprijed provjerena u pogledu pouzdanosti ili relevantnosti, niti je RCMP nametnuo bilo kakva ograničenja na njihovo korištenje. Kanadska istražna komisija potom je utvrdila da su ove informacije vjerovatno odigrale ulogu u pritvaranju Arara u Sjedinjenim Državama i njegovoj kasnijoj predaji Siriji, gdje je bio mučen. Ono što je ovdje bitno, komisija nije mogla doći do definitivnog nalaza zato što ni Vlada SAD-a, niti Sirijska vlada nisu sarađivala u istrazi. Suočeno sa zahtjevima očuvanja suvereniteta države, malo je toga što nadzorno tijelo može učiniti da prodre u dubine tajne međunarodne razmjene informacija. Ipak, i komisija u slučaju Arar i kasnija istraga o pritvaranju od strane Sirije i Egipta druge trojice Kanađana utvrdila je da su pitanja koja je RCMP i Kanadska sigurnosno-obavještajna služba poslali vlastima Sirije i Egipta doprinijela mučenju tih pritvorenika od strane sirijskih i egipatskih operativaca.

Takvi nalazi predstavljaju važna upozorenja o tome šta se mora izbjegavati. Oni upozoravaju da obavještajne i sigurnosne službe, čak i kada su suočene sa vanrednim okolnostima, moraju provjeriti informacije prije nego što ih dostave stranim partnerima. Također moraju, kada je to potrebno, priložiti upozorenja uz informacije i nametnuti ograničenja na njihovo korištenje. Nadalje, trebaju se uzdržavati od slanja naknadnih istražnih zahtjeva, kao što je spisak pitanja, stranim partnerima za koje se zna da u isljeđivanjima koriste mučenje ili druge oblike kršenja ljudskih prava.

3.2 DOBRE PRAKSE OBAVJEŠTAJNIH SLUŽBI U MEĐUNARODNOJ RAZMJENI INFORMACIJA

Šta je dobra praksa u pogledu međunarodne razmjene informacija? Za početak, agencije koje razmjenjuju informacije treba da osiguraju da su dobro obaviještene o partnerima sa kojima razmjenjuju informacije. Specijalni izvjestilac UN-a za promociju i zaštitu ljudskih prava i temeljnih sloboda prilikom borbe protiv terorizma preporučio je da „prije ulaska u sporazum o razmjeni informacija ili prije razmjene informacija na *ad hoc* osnovi, obavještajne službe treba da procjene kakva je situacija u pogledu zaštite ljudskih prava i podataka kod svog partnera, kao kakve su pravne garancije i institucionalne kontrole koje taj partner provodi. Prije nego što daju informacije, obavještajne službe treba da osiguraju da svaka razmijenjena informacija bude relevantna za mandat primaoca, da će biti korištena u skladu sa datim uslovima, te da neće biti korištena u svrhe kojima se krše ljudska prava."[12] Mada je specijalni izvjestilac ovu preporuku uputio obavještajnim službama, ona ima značaj i za nadzorna tijela čija je dužnost osigurati da se dobre prakse

primjenjuju, te da se osigura pravni lijek za svaki slučaj propuštanja primjene dobrih praksi.

Komisija u slučaju Arar ustanovila je da RCMP nije imao adekvatne informacije o praksi sirijskih i egipatskih sigurnosnih snaga kada je odlučila razmijeniti s njima informacije. Općenito govoreći, među agencijama koje razmjenjuju informacije na međunarodnom planu, policijske snage imaju najmanje stručnog znanja u procjenjivanju praksi stranih partnera. Bilo bi, stoga, mudro da domaće agencije, koje razmjenjuju sigurnosne informacije na međunarodnom planu, uspostave i čuvaju zajedničku bazu podataka aktualnih saznanja o potencijalnim stranim partnerima. Na taj način, domaće agencije mogu donositi odluke koje su zasnovane na dobroj obaviještenosti o specifičnoj razmjeni informacija. Takav pristup bi poboljšao proces odlučivanja ne samo u pogledu slanja informacija, već i procjene dobivenih informacija. U ranije navedenim kanadskim slučajevima, informacija koja je dobivena tokom surovog isljeđivanja kasnije je bila široko distribuirana među službenicima agencija za provedbu zakona, obavještajnih službi, te vanjskopolitičkih tijela. Kako je zaključila Komisija za slučaj Arar, „Nema smisla da različite agencije djeluju na osnovu različitih procjena informacija koje dobiju od inostrane vlade."[13]

Kao što je također ranije razmatrano, imperativ je da obavještajne i sigurnosne službe prilože upozorenja uz informacije koje dostavljaju stranim tijelima, te da nametnu odgovarajuća ograničenja na njihovo korištenje. Mada nema garancija da će strane vlade poštovati ta upozorenja, postoje dobre prakse koje mogu povećati vjerovatnoću da će ona biti poštovana. Usto, takve prakse mogu poboljšati šanse da će postojati pravni lijek u slučaju kršenja prava. Komisija za slučaj Arar je dala nekoliko preporuka u tom pogledu. Prvo, upozorenja treba da budu formulirana što jasnije i preciznije. Na primjer, dozvola vladi koja prima informacije da razmjenjuje te informacije unutar svoje „obavještajne zajednice" daje toj vladi preširok mandat s obzirom na brojne agencije koje se mogu uklopiti u jedan tako nejasan termin. Drugo, vladama koje primaju informacije treba općenito zabraniti korištenje razmijenjenih informacija u sudskim postupcima, bilo da su to krivični postupci, ili postupci vezani za imigraciju ili ekstradiciju. Nadalje, upozorenje treba uvijek da bude priloženo i u njemu treba da se traži od vlada koje primaju informaciju da kontaktiraju za to određene službenike vlade koja je poslala informaciju, ukoliko vlada koja je primila informaciju poželi da dopuni upozorenje, ili da prijavi zloupotrebu. To bi ispravilo sadašnju lošu praksu nejasnog formuliranja takvih upozorenja i njihovog upućivanja agencijama ili vladama koje su poslale informaciju, te bi promoviralo pojedinačnu odgovornost. Prema Komisiji za slučaj Arar, „upozorenje može poslužiti da se uspostave propisni kanali za jasnu komunikaciju o korištenju i distribuciji informacija koje su predmet upozorenja."[14] Konačno, treba uvijek uključiti upozorenje u kojem se zahtijeva da agencija koja prima informaciju poštuje kontrole ličnih informacija koje nameće zakon zemlje koja je poslala informacije, kao i kontrole zemlje koja prima informacije.[15]

Ukoliko sigurnosna agencija sazna da je jedno od njenih upozorenja bilo prekršeno, ona treba odmah uložiti žalbu agenciji koja je učinila prekršaj. Ovisno o ozbiljnosti prekršaja, agencija koja je proslijedila informaciju možda će trebati razmotriti opravdanost sporazuma o razmjeni informacija koji je poslužio kao osnova. Istovremeno, nadzorna tijela treba da budu obaviještena o svakom kršenju i odgovoru agencije koja je poslala informaciju. Nadzorna tijela mogu igrati važnu ulogu u osiguravanju da agencije koje nadziru zahtijevaju poštivanje upozorenja i da preduzimaju odgovarajuće radnje kada je to potrebno kako bi obezbijedile pravni lijek.

Kako se navodi u nalazima Komisije za slučaj Arar, posebnu pažnju treba posvetiti u

situaciji kada se šalju pitanja stranim agencijama, ne samo zato što ona mogu dovesti do korištenja grubih taktika u istrazi, već i zbog toga što strane agencije mogu koristiti takva pitanja na način koji je čak manje podložan kontroli koju podrazumijeva slanje upozorenja. "Informacije," zaključila je Komisija u slučaju Arar, "nikada ne treba da se pruže stranoj zemlji tamo gdje postoji uvjerljiv rizik da će to dovesti do, ili doprinijeti korištenju mučenja."[16] Specijalni izvjestilac UN-a je dao sličnu preporuku, uz naglasak da nadzorna tijela treba da budu posebno pažljiva prema aktivnostima koja mogu predstavljati kršenja ljudskih prava. Usto, on je preporučio da službenici obavještajnih službi kojima je naređeno da učestvuju u aktivnostima kojima se krše norme ljudskih prava treba da imaju ovlaštenje da odbiju takve naredbe i da ulože žalbe nadzornim tijelima u vezi s njima.[17]

Razmjena informacija sa stranim partnerima treba uvijek da bude dobro dokumentirana zbog rizika koje ona krije, te treba da omogući ocjenu i nadzor. Član 17. kanadskog Zakona o sigurnosno- obavještajnim službama daje ministru za javnu sigurnost (u konsultaciji sa ministrom vanjskih poslova) zakonsku ovlast da sklapa sporazume o saradnji sa stranim agencijama i vladama. U odsustvu takvog sporazuma, ova služba ne može zakonito dati informacije nekom stranom tijelu. Ona može, međutim, dobiti informacije.[18] Dodatna ministarska direktiva zahtijeva od RCMP-a da sklapa specifične pisane sporazume sa partnerima sa kojima razmjenjuje informacije. Tim sporazumima treba da prethodi konsultiranje zakona – a, u slučaju stranih agencija, konsultiranje Ministarstva vanjski poslova. Čak i kad se to obavilo, Komisija za slučaj Arar ustanovila je da RCMP nije primijenio ovu direktivu u svojoj dnevnoj razmjeni informacija. Komisija je zaključila da, mada „ne treba da budu nepotrebno formalni, niti predugi," pisani sporazumi mogu povećati osjetljivost agencije za potrebu da se prilikom razmjene informacija poštuju upozorenja i ljudska prava.[19]

Evidencija o obavljenoj ocjeni od posebnog je značaja kada neka sigurnosna agencija sklopi sporazum o saradnji sa stranim partnerom za kojeg se zna da ne poštuje ljudska prava. Kada se informacija dostavi takvom partneru, preporučuje Komisija za slučaj Arar, agencija koja pruža informaciju treba da sačini pisanu evidenciju u kojoj se opisuje razmijenjena informacija, te osnov za odluku o razmjeni.[20] Komisija dalje preporučuje da sličan pristup bude primijenjen i kada se dobija informacija iz zemalja sa upitnim stanjem ljudskim prava:

> *U pogledu odgovornosti, važno je da proces odlučivanja bude jasno opisan u pisanoj formi i da odgovornosti za donošenje odluka budu identificirane. Nadalje, odluke da se dobiju informacije od zemalja sa upitnim stanjem ljudskih prava treba da budu predmet provjere odgovarajućeg tijela.*[21]

3.3 DOBRE PRAKSE NADZORNIH TIJELA U MEĐUNARODNOJ BILATERALNOJ RAZMJENI INFORMACIJA

Od suštinskog je značaja da nadzorna tijela imaju pristup informacijama koje razmjenjuju agencije koje ona nadziru – bilo da ta informacija podrazumijeva tajnost ili ne. Među dobrim praksama koje preporučuje specijalni izvjestilac UN-a je da „nezavisne nadzorne institucije imaju mogućnost da razmotre sporazume za razmjenu informacija i svaku informaciju koju pošalju obavještajne službe stranim tijelima."[22] Zapravo, prema specijalnom izvjestitelju UN-a, „dobra praksa državnog zakonodavstva je da jasno zahtijeva od obavještajnih službi da podnose izvještaj o razmjeni informacija nezavisnoj nadzornoj instituciji."[23]

Jedna potencijalna prepreka učinkovitom nadzoru je pravilo treće strane, uobičajeno

upozorenje koje se stavlja na razmijenjene informacije koje ograničava njihovu distribuciju drugim tijelima („trećim stranama“). Neke zemlje, poput Njemačke, ne daju nadzornim tijelima pristup razmijenjenim informacijama zato što smatraju da su nadzorna tijela ta treća strana.

Ozbiljan odgovor na ovakvo tumačenje pravila o trećoj strani bilo bi da nadzorna tijela insistiraju da se, u slučaju međunarodne razmjene informacija, ona smatraju dijelom sigurnosne agencije koja dobiva strane informacije. Obavještajne službe se mogu oduprijeti takvom stavu u strahu da će zbog toga strane službe biti manje spremne razmjenjivati s njima informacije. Ali one mogu biti i ohrabrene da obavijeste svoje strane partnere o odgovornostima koje imaju u pogledu saradnje sa nadzornim tijelima, koja u mnogim slučajevima primjenjuju iste procedure tajnosti informacija, kao i agencija koja je dobila informacije.

Nadzorna tijela moraju također imati na umu da obavještajne službe nekada koriste razmjenu informacija kao sredstvo izbjegavanja domaćih ograničenja za svoje aktivnosti. U vezi sa ovim problemom, specijalni izvjestilac UN-a predložio je dobru praksu zasnovanu na izvještaju Evropskog parlamenta o sistemu za presretanje komunikacija ECHELON: „obavještajnim službama (je) zabranjeno da koriste pomoć stranih obavještajnih službi na bilo koji način koji rezultira izbjegavanjem domaćih pravnih standarda i institucionalnih kontrola njihovih vlastitih aktivnosti.”[24]

Konačno, nadzorna tijela treba da usvoje i/ili podstiču iste dobre prakse razmjene informacija koje se preporučuju obavještajnim službama za koje su zadužene. Na primjer, nadzorna tijela treba da se obavijeste o tome kako strani partneri poštuju ljudska prava. Slično tome, one treba da ohrabre agencije koje nadziru da sklope formalne pisane sporazume sa svojim stranim partnerima.

Okvir 3: Nadzor Holandskog odbora za ocjenu rada obavještajnih i sigurnosnih službi u međunarodnoj razmjeni informacija

Holandska vlada je 2002. godine osnovala stalno tijelo - Odbor za ocjenu rada obavještajnih i sigurnosnih službi - sa odgovornošću da nadzire cijeli niz obavještajnih pitanja, uključujući tu i nadležnost za ocjenjivanje rada nekoliko obavještajnih agencija, te joj je omogućila pristup tajnim informacijama koji je potreban za obavljanje tog posla. Ovaj Odbor je 2009. godine izdao opsežan izvještaj o holandskoj saradnji sa stranim službama koji je usmjeren na politike i prakse Holandske obavještajne službe za period od 2002. i sredine 2005. godine.

U izvještaju se navodi da holandska služba i njen odjel za vanjske poslove nisu bili dovoljno pažljivi u pogledu toga da li su strani partneri, uključujući one sa lošim stanjem ljudskih prava, zadovoljavali odgovarajući standard razmjene informacija. U izvještaju se također navodi da su holandske obavještajne službe djelovale nezakonito kad su davale lične informacije stranim partnerima. Ona je preporučila da te službe prestanu razmjenjivati informacije sa stranim partnerima za koje sumnjaju da bi mogli te informacije koristiti u nezakonite svrhe.[25] Izvještaj, također, preporučuje da se uspostavi strukturirani proces utvrđivanja da li treba sklopiti sporazum o razmjeni informacija sa nekom stranom službom, ili ne. Takvi sporazumi treba da budu predmet periodičnih ocjena, te bi obavezali da se čuva pisana evidencija o svim razmijenjenim ličnim informacijama.[26]

3.4 DOBRE PRAKSE NADZORNIH TIJELA U POGLEDU MEĐUNARODNE RAZMJENE INFORMACIJA PUTEM MREŽA

Pošto se međunarodna razmjena informacija može odvijati i multilateralno i bilateralno, nadzorna tijela treba da se postave tako da mogu na najmanju moguću mjeru svesti izazove, a na maksimum svesti prilike koje sobom nosi razmjena informacija putem mreža. Na primjer, mreže za razmjenu informacija mogu vršiti procjene poštivanja ljudskih prava partnerskih agencija na način koji može biti prihvatljiviji od oslanjanja na to da pojedine članice mreže rade iste takve procjene. Mreže mogu također imati veći utjecaj na pojedinačne agencije kada se radi o provedbi upozorenja u pogledu ljudskih prava i privatnosti, koji idu uz brojne razmjene informacija.[27] Konačno, mreže imaju potencijal da šire dobre prakse u pogledu pouzdanosti informacija i nadzora, time što zahtijevaju od članica da ispunjavaju standarde koje su uspostavile druge članice koje primjenjuju najbolje prakse.

Neke evropske mreže za razmjenu informacija, kao što su one kojima upravlja Europol i Bernski klub, doista su nametnule visoke standarde i oni su se pokazali korisnim. Međutim, one su također ohrabrile neke države da se odluče za manje formalnu (a čak i od slučaja do slučaja) bilateralnu razmjenu informacija.[28] Kako bi se suprotstavila toj tendenciji, nadzorna tijela treba da primijene dvosmjerni pristup, naglašavajući koristi razmjene informacija u okviru multilateralnih mreža, dok se istovremeno posvećuje velika pažnja razmjeni informacija koja se odvija u sklopu manje transparentnih bilateralnih aranžmana. Mada može biti teško dobiti informacije o stranim partnerima sa kojima domaća obavještajna služba razmjenjuje informacije, nadzorna tijela treba da dobiju te informacije i prate primjenu sporazuma i praksi u međunarodnoj razmjeni informacija.

Za zemlje u razvoju, resursi koji su na raspolaganju članicama međunarodnih mreža za razmjenu informacija pružaju snažan poticaj da se pridruže, čak i ako pridruživanje zahtijeva poštivanje određenih standarda ljudskih prava. Nadzorna tijela mogu igrati važnu ulogu u promociji članstva tako što će se obavijestiti o standardima koje treba ispuniti, te obavještajne i sigurnosne službe koje nadziru ohrabrivati da ih i ispunjavaju.

4. NADZOR NAD RAZMJENOM INFORMACIJA SA DOMAĆIM AGENCIJAMA

Kao što je ranije razmatrano, nakon napada 11. septembra, mnoge vlade su povećale razmjenu informacija među domaćim partnerima – uključujući obavještajne, policijske, granične, carinske i transportne službenike – u uvjerenju da će tako povećana razmjena informacija pomoći u sprječavanju budućih terorističkih napada. U Ujedinjenom Kraljevstvu, na primjer, Član 19. Zakona o terorizmu iz 2008. godine dao je obavještajnim službama Ujedinjenog Kraljevstva široki prostor u pogledu razmjene informacija. Posebno je dao saglasnost na otkrivanje informacija obavještajnim službama od strane bilo koje osobe. Također je ovlastio obavještajne službe da otkriju informacije kada je to potrebno radi ispravnog obavljanja njihove funkcije, radi sprječavanja ili otkrivanja ozbiljnih krivičnih djela te u svrhu krivičnih postupaka. Na taj način, nedavni pritisak da se poveća razmjena informacija rezultirao je velikom razmjenom informacija vezanim ne samo za potencijalne sigurnosne prijetnje već također i u pogledu sprječavanja kriminala i krivične istrage.

4.1 IZAZOVI ZA DOMAĆU RAZMJENU INFORMACIJA

Iz perspektive nadzora, otkrivanje informacija domaćim partnerima otvara ista ona brojna pitanja koja su razmatrana ranije u vezi sa međunarodnom razmjenom informacija. Ima nekih dodatnih pitanja, međutim, koja su vezana specifično za domaću razmjenu informacija. Najvažnije od tih pitanja je opasnost da ograničenja u pogledu nadležnosti mogu spriječiti učinkovitu, koordiniranu ocjenu domaće razmjene informacija, pošto nadzorna tijela koja su u to uključena nemaju pravnu ovlast da provjeravaju sve uključene domaće agencije. Kada ne postoje nadzorne ovlasti u ovom pogledu, odgovornost je razblažena te nastaje rupa u kojoj se razmjena informacija može vršiti bez adekvatne ocjene.

Pošto obavještajne službe posjeduju posebne ovlasti, vlade država obično ih podvrgavaju većem stepenu nadzora od onog koji je nametnut agencijama za provedbu zakona. Kada dođe do jaza u odgovornosti, taj povećan nadzor može biti podriven. Na primjer, kada je Kanadska vlada odlučila istražiti akcije kanadskih službenika u pogledu mučenja u predmetu Mahera Arara i drugih Kanađana u Siriji i Egiptu, ustanovila je da se nadležnost stalnog Odbora za ocjenu sigurnosnih i obavještajnih službi nije odnosila na službenike policije, carine, vanjskih poslova i za imigraciju koji su bili uključeni u razmjenu informacija sa Sirijom i Egiptom. Kao rezultat, morala je pokrenuti *ad hoc* istrage kako bi ispunila tu prazninu u utvrđivanju odgovornosti.

Federalizam također može dovesti do opasnih prazninu u utvrđivanju odgovornosti. U Sjedinjenim Državama nakon 11. septembra, na primjer, formirani su centri za fuziju radi promocije razmjene informacija između saveznih, državnih i općinskih agencija. Zagovornici ovog rešenja su insistirali da nisu bili potrebni novi nadzorni mehanizmi zato što svaka agencija koja učestvuje u tom procesu je i dalje bila podložna već postojećoj strukturi nadzora. Taj argument, međutim, ne prepoznaje činjenicu da, u praksi, nadzorna tijela vezana za jedan nivo vlasti rijetko imaju nadležnost potrebnu da ocjenjivali akcije koje preduzmu agencije na drugim nivoima vlasti.[29]

4.2 LOŠE PRAKSE U DOMAĆOJ RAZMJENI INFORMACIJA

Od 11. septembra, jedna posebno loša praksa u domaćoj razmjeni informacija je pogrešna identifikacija nenasilnih demonstranata kao osumnjičenih za terorizam. U Sjedinjenim Državama, nekoliko centara za fuziju je optuženo za takve prakse. Pogrešna identifikacija se desila nakon što su razne baze podataka, koje su obezbijedile savezne, državne i lokalne agencije bile spojene sa strateškim informacijama vezanim za terorističke prijetnje i ranjivosti. Agencije koje su učestvovale u tome ili su tvrdile da nisu znale za to ili su krivile nekog drugog za nepouzdane informacije. Neki centri za fuziju su otežali problem time što su odbili predati nadzornim tijelima evidenciju u kojoj su opisani načini na koje su objedinjene informacije.[30] Ti faktori zajedno umanjuju odgovornost centara za fuziju i agencija koje u njima učestvuju za njihove aktivnosti.

Općenitije govoreći, informacijske mreže i agencije koje im pripadaju trebaju smanjiti nasumičnu razmjenu potencijalno nepouzdanih informacija. U Kanadi, nepouzdane informacije koje je od jedne strane agencije dobilo Ministarstvo vanjskih poslova bile su kasnije proslijeđene domaćim obavještajnim službama i agencijama za provedbu zakona, a da nije data bilo kakva napomena u pogledu pouzdanosti. Čak su te informacije bile korištene i kao osnov za dobivanje naloga za pretres. Na taj način, loše prakse u domaćoj razmjeni informacija mogu umnožiti opasnosti koje su svojstvene u međunarodnoj razmjeni informacija.

4.3 DOBRE PRAKSE U DOMAĆOJ RAZMJENI INFORMACIJA

Dobre prakse u domaćoj razmjeni informacija počinju sa čuvanjem stalne evidencije u kojoj se prati trag informacija koje se čuvaju i koje su razmijenjene sa centrima za fuziju i drugim tijelima koja omogućavaju razmjenu informacija. Bez vođenja takve evidencije i revizorske dokumentacije, nadzor nad domaćom razmjenom informacija bi bio težak, ako ne i nemoguć.

Upozorenja pri razmjeni informacija su jednako dobra praksa kako u domaćoj tako i u međunarodnoj razmjeni informacija, pogotovo kada će se razmijenjena informacija koristiti u vezi sa provedbom zakona. Agencija koja razmjenjuje informacije treba pažljivo razmotriti da li su razmijenjene informacije dovoljno pouzdane da se koriste u svrhu provedbe zakona, te, također, da li agencija ima zakonsko pravo da razmjenjuje informacije u tu svrhu. Specijalni izvjestilac UN-a je naglasio potrebu da zemlje usvoje pravni osnov za domaću razmjenu informacija. Član 19. Zakona o terorizmu Ujedinjenog Kraljevstva iz 2008. godine pruža takav jedan primjer.

Stvaranje pravnog osnova može zakonodavcima pružiti priliku da razmotre valjanost mehanizama nadzora koji su trenutno na snazi i da možda uvedu promjene u pogledu aktualne strukture nadzora. Na primjer, dok je razmatrala pravni osnov za nadzor u Kanadi, Komisija za slučaj Arar preporučila je kanadskom zakonodavcu da stvori pravnu osnovu kojom će se omogućiti različitim nadzornim tijelima da razmjenjuju tajne informacije i zajedno rade na ocjeni državnih sigurnosnih aktivnosti. Ova preporuka Komisije se zasnivala na dobrom principu da nadzor treba da drži korak sa aktivnostima koje se nadziru. Drugim riječima, ako se zakonsko ovlaštenje za razmjenu informacija proširi, tada se također moraju proširiti ovlasti za njihovu ocjenu

Komentatori tvrde da je jedan zaseban oblik „odgovornosti mreže“ neophodan ako nadzorna tijela žele održati korak sa povećanjem broja domaćih mreža za razmjenu informacija. Preporuke uključuju registriranje i čuvanje svih razmijenjenih informacija (tako da nadzorna tijela mogu prikupiti evidencije na osnovu kojih je moguće raditi naknadne revizije), te uspostavu mehanizama unošenja ispravke u okviru centara za fuziju (tako da prosljeđivanje netačnih informacija i kršenja prava privatnosti može biti ispravljena).[31] Ostali komentatori naglašavaju potrebu za postojanje službe generalnog inspektora, posebno u Sjedinjenim Državama, koji bi provodio zajedničke istrage o praksama razmjene informacija agencija koje oni nadziru.[32] U Kanadi, Komisija za slučaj Arar slično je preporučila da nadležnost nadzornih tijela nad sigurnosnim službama bude proširena tako da uključi jedan broj agencija koje su preuzele na sebe značajne nove sigurnosne zadatke nakon 11. septembra. [33]U Belgiji, zasebna tijela koja nadziru policiju i obavještajne službe, koja već imaju dozvolu da razmjenjuju informacije, također su provela nekoliko zajedničkih istraga.[34]

U odsustvu tako širokih rješenja za nadzor, vlade koje žele da istraže akcije više domaćih agencija koje su angažirane u razmjeni sigurnosnih informacija moraju uspostavljati *ad hoc* istrage, kao što je to bila Komisija za slučaj Arar, pošto nijedno postojeće nadzorno tijelo nema potrebni mandat da provjerava akcije više agencija istovremeno. Imenovanje takvog *ad hoc* tijela, međutim, ne može biti zamjena za stalno nadzorno tijelo sa dovoljnim ovlaštenjima da obavlja propisnu ocjenu rada službi. Iz tog razloga, Komisija za Arar je preporučila da stalna nadzorna tijela, zadužena za ocjenu rada kanadskih obavještajnih agencija i agencija za provedbu zakona, dobiju veće ovlasti koje će im omogućiti da provjeravaju akcije jednog broja agencija sa kojima se sigurnosne informacije razmjenjuju.

Na žalost, ova preporuka i preporuka da vlada stvori zakonske pretpostavke za zajednički nadzor – obje date 2006. godine – tek treba da budu provedene.[35]

U Sjedinjenim Državama je izvjestan napredak postignut u pogledu prijenosa trajne odgovornosti na organe i institucije koje imaju kapacitete da vrše ocjenu rada više domaćih agencija koje sada učestvuju u razmjeni sigurnosnih informacija. Jedan primjer je istraga prisluškivanja telefona koje je urađeno bez naloga, koju su zajedno proveli generalni inspektori Ministarstva odbrane i Ministarstvo pravde, Centralna obavještajna agencija, Agencija za državnu sigurnost i Ured direktora za državne obavještajne službe.[36]

Okvir 4: Ocjena domaće razmjene informacija putem istrage australijskih obavještajnih službi

Australija je postigla značajan napredak u prilagođavanju nadzora nad obavještajnim službama kako bi se odgovorilo na novi pristup sigurnosnim pitanjima i razmjeni informacija koji se odnosi na cijelu vladu. Australijska istraga obavještajnih agencija preporučila je 2006. godine da generalni inspektor, stručno nadzorno tijelo i parlamentarni zajednički odbor dobiju proširene mandate kojim bi im se omogućilo da nadziru akcije svih domaćih obavještajnih agencija.[37]

Mada ova preporuka priznaje da se proširila razmjena informacija među domaćim obavještajnim službama, manje pažnje je posvetila razmjeni informacija između domaćih obavještajnih službi i drugih domaćih agencija. Ovaj nedostatak je ispravljen 2010. godine, kada je australijski parlament usvojio zakon koji je generalnom inspektoru dao ovlast da razmatra sva pitanja vezana za sigurnost i obavještajni rad unutar bilo kojeg saveznog ministarstva ili agencije.[38] U jednom pogledu, međutim, taj novi zakon je manje postigao od onog što se željelo. Mada je specijalni izvjestilac UN-a naglasio značaj činjenice da nadzorna tijela moraju biti u stanju pokrenuti vlastite istrage, novi australijski zakon zahtijeva da premijer odobri istrage generalnog inspektora.[39]

U međuvremenu, Australija je osnovala nove parlamentarne odbore radi ocjene akcija agencija za provedbu zakona koje su uključene u državnu sigurnost i razmjenu informacija. Također je proširila sastav zajedničkog parlamentarnog odbora zaduženog za nadzor nad obavještajnim službama.

5. PREPORUKE

Sljedeće preporuke imaju namjeru olakšati nadzor nad domaćom i međunarodnom razmjenom informacija. One su upućene ne samo nadzornim tijelima u zakonodavnoj i izvršnoj vlasti, već i obavještajnim službama koje se nadziru i raznim drugim tijelima uključenim u cjelokupni odgovor vlasti na sigurnosne prijetnje.

S obzirom da mora postojati, razmjena informacija mora biti vođena na način koji je zakonski zasnovan, te mora poštovati ljudska prava, uključujući pravo na privatnost. Važno sredstvo da se to postigne je da se nadzornim tijelima zakonima daju ovlaštenja i resursi potrebni kako bi održali korak sa sve većim intenzitetom domaće i međunarodne razmjene informacija u svijetu nakon 11. septembra.

Izrada internih smjernica za razmjenu informacija

Obavještajne službe treba da osmisle set principa kojim će se rukovoditi njihove prakse razmjene informacija. Ti principi treba da budu utvrđeni u pisanom obliku, bilo kao zakon ili kao politika. Oni treba da:

- nametnu obavezu poštivanja ljudskih prava (uključujući zabranu saučesništva u mučenju) i poštivanje zakona koji se odnose na zaštitu privatnosti (uključujući razmjenu ličnih informacija). Ovi principi posebno treba da zabranjuju razmjenu informacija tamo gdje postoji stvarni rizik da će razmjena informacija izazvati ili doprinijeti praksi mučenja;
- zahtijevaju provjeru razmijenjenih informacija (bilo da je poslana ili primljena) u pogledu relevantnosti, pouzdanosti, tačnosti i utjecaja na privatnost i druga ljudska prava.
- priznaju potrebu da se prilože upozorenja uz informacije koje se šalju, te da se upozorenja drugih poštuju za dobivene informacije – svrha ovih upozorenja je da se osigura da se razmijenjena informacija ne koristi u nepropisne svrhe, niti na nepropisan način koji krši domaće i međunarodne zakone;
- prepoznaju i obavezu da se isprave pogrešne informacije koje su poslane drugim agencijama, te da provode nezavisne procjene pouzdanosti informacija dobivenih od drugih;
- uključe obavezu razmjene informacija na način koji olakšava poštivanje odgovornosti unutar službe koja ih razmjenjuje i u pogledu nadzornih tijela. To znači da razmijenjena informacija treba biti registrirana u pisanoj formi, te da evidencije treba da uključe opis kako je informacija razmijenjena kao i bilo koje daljnje prakse. Ako se razmjena informacija obavlja bez takvog ovlaštenja – na bilo kojem terenskom nivou, ili u izuzetnim okolnostima – to treba da bude jasno objašnjeno u pisanoj formi i to što je moguće prije.

Obavještajne službe treba da ove principe uključe u svoje programe obuke te ih razmijene sa nadzornim tijelima. One također treba da ih daju na raspolaganje javnosti, pod uslovom da se ne otvaraju pitanja povjerljivosti u pogledu državne sigurnosti. Ako obavještajna služba propusti da definira ove principe, njeno nadzorno tijelo treba da definira slične principe i primjenjuje ih u svom nadzornom radu.

Razvoj pristupa razmjeni informacija unutar obavještajne službe koji se zasniva na punoj obaviještenosti

Obavještajne službe treba da čuvaju baze podataka koje prate evidenciju o ljudskim pravima u zemljama sa kojima razmjenjuju informacije. Te baze podataka treba da:

- uključe široki spektar otvorenih informacija, uključujući navode o kršenjima ljudskih prava koja iznesu međunarodna i regionalna tijela za zaštitu prava, te uvažene grupe civilnog društva;
- budu izrađene u konsultaciji sa ministarstvom vanjskih poslova;
- se koriste za obuku službenika obavještajne službe;
- se stave na raspolaganje javnosti na način koji nije u suprotnosti sa pitanjima državne povjerljivosti u pogledu državne sigurnosti.

Nadzorna tijela treba da imaju pristup ovim bazama podataka – koje oni treba da revidiraju i, kada je to potrebno, dopune i ažuriraju. Ako obavještajne službe ne uspiju stvoriti takvu jednu bazu podataka, njihova nadzorna tijela trebaju to učiniti.

Izrada međunarodnih sporazuma o razmjeni informacija

Obavještajne službe treba da sačine pisane sporazume za upravljanje razmjenom informacija sa stranim partnerima. Ti sporazumi treba posebno da navedu obaveze strane koja šalje i strane koja prima informacije u pogledu ljudskih prava. Oni također treba da uključe standardne klauzule koje omogućavaju da dobivena informacija bude razmijenjena sa glavnim nadzornim tijelom date službe i, gdje je to moguće, sa sličnim nadzornim tijelima koja se saglase sa istim protokolima povjerljivosti. U izradi ovih sporazuma, obavještajna služba treba da dobije i pravni i vanjskopolitički savjet.

Nadzorna tijela treba da dobiju primjerke svih takvih sporazuma u trenutku kada stupe na snagu ili kada su revidirani. Nadzorno tijelo mora biti obavezno da razmotri svaki sporazum i, gdje je to moguće, provede nasumične provjere kako bi se utvrdilo da li se poštivaju uslovi tih sporazuma. Takve ocjene mogu pomoći da se utvrdi da li sporazum treba revidirati u svjetlu prethodne prakse.

Prijavljivanje i rješavanje kršenja upozorenja koja se daju uz razmijenjenu informaciju

Sporazumi o razmjeni informacija treba da uključe specifične procedure za prijavljivanje kršenja upozorenja koja se prilažu uz razmijenjenu informaciju strana koja šalje informacije, te rješenje sporova koji proizlaze iz kršenja upozorenja. Ako agencija koja šalje informacije sazna za kršenje, ona treba da uputi formalni prigovor agenciji koja prima informacije. Agencija koja šalje informaciju treba također da ovo iskoristi kao priliku da ponovno razmotri dati sporazum o razmjeni informacija te možda da unese i izmjene. Takva procedura može se također koristiti za ispravku ili ažuriranje informacija te za predlaganje dopuna uz upozorenja u specifičnim slučajevima ili nakon izvjesnog vremena.

U slučaju kršenja (ili čak sumnje na kršenje), obavještajne službe treba o tome da obavijeste svoja nadzorna tijela. Takve obavijesti treba da uključe bilješku o bilo kakvoj radnji za ispravku situacije koju je služba preduzela ili predlaže za preduzimanje. Nadzorno tijelo treba da razmotri i da komentar na sve radnje ispravke te također da odgovori na generalno pitanje kako će to kršenje utjecati na buduću razmjenu informacija sa partnerom koji je prekršio sporazum.

Izvještavanje i rješavanje nezakonitog korištenja razmijenjene informacije

Obavještajne službe treba da obavijeste svoja nadzorna tijela kada saznaju (ili čak sumnjaju) da je razmijenjena informacija dobivena, ili se koristi, ili bi mogla biti korištena nezakonito, posebno u pogledu kršenja ljudskih prava. Takve obavijesti treba da sadrže i zabilješke o svakoj ispravci koju je služba preduzela ili koju predlaže preduzeti. Nadzorno tijelo treba razmotriti i dati komentar na sve ispravke, te odgovoriti na generalno pitanje kako će to kršenje utjecati na buduću razmjenu informacija sa partnerom koji je prekršio sporazum.

Izrada domaćih sporazuma o razmjeni informacija

Obavještajne službe treba da izrade pisane sporazume kojim se rukovodi u razmjeni informacija sa domaćim partnerima. Takvi sporazumi treba da:

- budu nedvosmisleno zasnovani na zakonu;
- sadrže obavezu upozorenja, kao i da poštuju ljudska prava;
- obavežu vođenje revizorske dokumentacije (uključujući stalnu evidenciju o svim informacijama koje su razmijenjene i pisanim ovlaštenjima agencija koje su slale i koje su primale informaciju);
- reguliraju kako će domaća razmjena informacija biti razmatrana od strane relevantnih nadzornih tijela.

U izradi ovih sporazuma, obavještajna služba treba da dobije pravni savjet, posebno u pogledu privatnosti i drugih zakonskih ograničenja na razmjenu informacija. Pravni savjet treba također da odgovori na pitanje da li je nadležnost nadzornog tijela te agencije dovoljna za provjeru njenih praksi razmjene informacija.

U pogledu rješavanja pitanja odgovornosti, ovi sporazumi treba da predvide i riješe problem koji nastaje zbog činjenice da agencije koje šalju i agencije koje primaju informacije mogu biti podložne različitim režimima nadzora. Gdje god je to moguće, tijela za nadzor treba da dobiju pristup svim informacijama potrebnim za učinkovitu ocjenu praksi razmjene informacija. To može zahtijevati dodatne zakonske izmjene kako bi se domaćim nadzornim tijelima omogućilo da provode zajedničke ocjene i razmjenjuju međusobno informacije. Ovaj zadatak nadzornih tijela, također, može zahtijevati od njih da se pridržavaju strožijih sigurnosnih mjera i mjera tajnosti nego što je to njihova uobičajena praksa.

Bilješke

1. Termin *obavještajna služba* se koristi ovdje u značenju vladine organizacije čiji glavni zadaci su prikupljanje i analiza informacija vezanih za državnu sigurnost, i njihova diseminacija onima koji donose odluke. Ova definicija je preuzeta iz knjige Aidana Willsa, *Guidebook: Understanding Intelligence Oversight*, Toolkit—Legislating for the Security Sector (Geneva: DCAF, 2010), str. 10.
2. BBC News, "Libya: Gaddafi regime's US-UK spy links revealed," 3. septembar 2011. (dostupno na http://www.bbc.co.uk/news/world-africa-14774533).
3. James Walsh, "Intelligence-Sharing in the European Union: Institutions Are Not Enough," *Journal of Common Market Studies* Vol. 44, izdanje 3 (September 2006), str. 625–643.
4. Elizabeth Sepper, "Democracy, Human Rights and Intelligence Sharing," T*exas International Law Journal* Vol. 46 (2010), str. 155.
5. Ernest R. May (uredn.), T*he 9 /11 Commission Report* (New York: St. Martins Press, 2007), Dio 3.2.
6. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (2010).
7. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006); i Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008).
8. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), str. 331.
9. Detainee Inquiry, "Protocol for the Detainee Inquiry" (2011) (dostupno na http://www.detaineeinquiry.org.uk/key-documents/protocol/).
10. Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, br. 3 (Proljeće 2007), str. 674.
11. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A NewReview Mechanism for the RCMP's National Security Activities* (2006), str. 431.
12. United Nations Human Rights Council, (Vijeće UN-a za ljudska prava), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010), str. 46.
13. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), str. 349.
14. Ibid., str. 342.
15. Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* (Geneva: DCAF, Univerzitet Durhama, i Parlament Norveške, 2005), str. 45.
16. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), str. 345.
17. United Nations Human Rights Council, (Vijeće za ljudska prava UN), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010).
18. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), str. 82.
19. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), str. 322.
20. Ibid., str. 347.
21. Ibid., str. 348.
22. United Nations Human Rights Council (Vijeće za ljudska prava UN), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010), str. 48.
23. Ibid., str. 49.
24. Ibid., str. 49–50.
25. Holandija, Review Committee on the Intelligence

and Security Services (CTIVD), *Review Report on the cooperation of the GISS with foreign intelligence and/or security services*, CTIVD No. 22A (12. avgust 2009) (dostupno na http://www.ctivd.nl/?English), Dio 14.2.

26. Ibid., Dijelovi 14.6 i 14.15.
27. Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, br. 3 (Proljeće, 2007), str. 683–684.
28. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), str. 68.
29. Danielle Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* Vol. 62 (2011), str.1441.
30. Ibid.
31. Ibid.
32. Philip Heymann i Juliette Kayyem, *Preserving Liberty in the Face of Terror* (Boston: MIT Press, 2005); Kent Roach, "Review and Oversight of National Security Activities and Some Reflections on Canada's Arar Inquiry," *Cardozo Law Review* Vol. 29, Issue 1 (oktobar 2007), str. 53–84.
33. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A NewReview Mechanism for the RCMP's National Security Activities* (2006).
34. Ibid., str. 333–334.
35. Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge: Cambridge University Press, 2011), str. 416–420 i 455–459.
36. Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program* (10. juli 2009).
37. Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Vlada Australije, 2004).
38. Australija, National Security Legislation Amendment Act No. 127 iz 2010, shema 9; vidjeti također Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (New York: Cambridge University Press, 2011), str. 354–356.
39. United Nations Human Rights Council, (Vijeće za ljudska prava UN), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, United Nations Document A/HRC/14/46 (17. maj 2010).

POGLAVLJE 8

Finansijski nadzor nad obavještajnim službama

Aidan Wills

OSAM

8

Finansijski nadzor nad obavještajnim službama

Aidan Wills[1]

1. UVOD

U demokratskim zemljama, parlamenti raspodjeljuju sredstva iz trezora javnim agencijama, kako bi mogle obavljati svoju funkciju i ispunjavati svoj zakonski mandat. Parlamenti, potom, zajedno sa drugim nadzornim tijelima, prate trošenje tih sredstava kako bi osigurali da njihovo korištenje bude i zakonito i djelotvorno. Sve javne agencije se moraju podvrgnuti ovom procesu, uključujući i obavještajne službe.

Ovo poglavlje predstavlja komparativni pregled kako domaća politička tijela nadziru finansije obavještajnih službi, od izrade budžeta do naknadne (*ex post)* ocjene njegove potrošnje. Cilj joj je da naglasi dobre prakse. Tekst sadrži sljedećih šest dijelova:

- *Značaj finansijskog nadzora nad obavještajnim službama* - objašnjenje zašto je vanjski nadzor važan;
- *Budžeti za obavještajni rad* - pregled različitih pristupa izradi budžeta za obavještajni rad;
- *Mehanizmi unutarnjih finansijskih kontrola i revizija* - pregled kontrola i mehanizama koji vanjski nadzor čine učinkovitijim;
- *Parlamentarni nadzor* - diskusija o ulozi parlamenata u izradi budžeta za obavještajni rad, nadzor nad njegovom provedbom, te praćenje potrošnje u službi u smislu legalnosti i učinkovitosti;

- *Glavne revizorske institucije* - diskusija o ulozi glavnih revizorskih institucija (GRI) u reviziji finansija obavještajnih službi;
- *Preporuke* - zbir dobrih praksi koje se odnose na finansijski nadzor nad obavještajnim službama

Zbog ograničenog prostora, ovo poglavlje se ne bavi ulogama koje u finansijskom nadzoru nad obavještajnim službama vrše izvršna vlast, generalni inspektor, tužioci i sudstvo.

2. ZNAČAJ FINANSIJSKOG NADZORA NAD OBAVJEŠTAJNIM SLUŽBAMA

Četiri su glavna razloga zašto je vanjski nadzor nad finansijama obavještajnih službi važan:

- Principi demokratskog upravljanja nalažu da se korištenje javnih sredstava pažljivo kontrolira.
- Finansijska evidencija može dati uvid u aktivnosti i rad obavještajnih službi.
- Tajnost rada obavještajnih službi ograničava sposobnost javnosti da kontrolira njihove aktivnosti.
- Priroda obavještajnog rada nosi sa sobom cijeli niz raznih finansijskih rizika, uključujući i rizik zloupotrebe javnih sredstava.

2.1 DEMOKRATSKO UPRAVLJANJE NAD KORIŠTENJEM JAVNIH SREDSTAVA

Opšteprihvaćeni princip demokratskog upravljanja je da raspodjelu finansijskih sredstava moraju odobriti izabrani predstavnici naroda – odnosno parlament – zato što novac koji se raspodjeljuje pripada narodu. Jednako važna je činjenica da javna potrošnja mora biti podložna naknadnoj provjeri koju vrše parlament i nezavisna tijela koja podnose izvještaj parlamentu, kao što je glavna revizorska institucija. Svrha naknadne ocjene je da se osigura, između ostaloga, da:

- se javna sredstva koriste u svrhe za koje su prvobitno raspoređena;
- potrošnja mora biti usklađena sa odgovarajućim zakonom (uključujući i zakone o upravljanju javnim sredstvima, zakone o javnim nabavkama, zakone o borbi protiv korupcije, te zakone kojim se reguliraju aktivnosti tijela koja vrše potrošnju);
- potrošnja mora biti u skladu sa politikama vlada;
- potrošnja pruža najvišu vrijednost za uloženi novac (eng. value for money) time što se na učinkovit način postižu utvrđeni ciljevi.

Mada se ovi principi primjenjuju jednako na sve vladine agencije, uključujući i obavještajne službe, neke zemlje jasno isključuju obavještajne službe iz određenih zakona kojim se regulira potrošnja javnih sredstava. U tim slučajevima, kao što je onaj u Sjedinjenim Državama u vezi sa Centralnom obavještajnom agencijom (CIA),[2] pažljiva kontrola je osobito važna.

2.2 FINANSIJSKA EVIDENCIJA KAO POKAZATELJ AKTIVNOSTI I UČINKA

Finansije javnih agencija obično u velikoj mjeri pokazuju koje su njene aktivnosti i učinak. Rijedak je slučaj da agencija može obavljati svoj zadatak a da pritom ne troši novac. Stoga,

njene finansijske evidencije često kriju „ključ“ za skrivene aktivnosti, uključujući neke koje mogu biti i nezakonite. U slučaju obavještajnih službi, nezakonite aktivnosti, kao što su djelovanje tajnih pritvorskih jedinica i prikriveno finansiranje domaćih političkih partija, mogu se otkriti u finansijskoj evidenciji date službe. Slično, neobično visoka budžetska linija određenog odsjeka može biti indikator lošeg učinka tog odsjeka. Stoga, ocjenjivanjem finansijske evidencije službe tijela za nadzor mogu identificirati aspekte rada službe koji možda nalažu daljnju kontrolu.

2.3 TAJNOST I OGRANIČAVANJE JAVNE KONTROLE

Pošto obavještajni rad zahtijeva neobično visok nivo tajnosti, finansije obavještajne službe ne otkrivaju se u istom stepenu kao informacije drugih vladinih agencija. Uz tajnost vezanu za tenderske procedure za nabavku robe i ugovaranje usluga[3] ide i činjenica da su obavještajne službe isključene iz većine zakona kojima se regulira pristup javnosti informacijama u posjedu države, što ograničava količinu relevantnih informacija koje mediji i organizacije civilnog društva mogu dobiti. S obzirom na ova ograničenja u pogledu javne kontrole, posebno je važno da vanjska tijela za nadzor koja imaju pristup povjerljivim informacijama mogu pažljivo kontrolirati finansije obavještajne službe.

2.4 UPRAVLJANJE FINANSIJSKIM RIZIKOM U OBAVJEŠTAJNOM RADU

Posebni aspekti obavještajnog rada nose sa sobom veći rizik da će javna sredstva biti korištena neučinkovito ili nepropisno. Mnogi od tih aspekata također otežavaju nadzor nad obavještajnim službama.

2.4.1 Neizvjesni rezultati

Obavještajne službe prikupljaju informacije kako bi pomogle kreatorima politika na planu zaštite državne sigurnosti. Da bi obavile ovu funkciju, službe troše novac, ali one nikada ne mogu ni same biti sigurne da će novac koji potroše polučiti informacije za kojima tragaju. Na primjer, određena služba može potrošiti velika sredstva na vrbovanje stranog doušnika da bi na kraju otkrila da taj doušnik posjeduje malo vrijednih informacija. Mada su takvi rizici svojstveni obavještajnom radu, unutarnje kontrole i vanjski nadzor mogu njima upravljati, čime se na najmanju mjeru svodi bespotrebno trošenje javnih sredstava.

2.4.2 Neopipljive koristi

Mada su finansijski troškovi jedne obavještajne operacije često opipljivi, koristi koju ona donosi su često neopipljive. Kao što je zapazio glavni kanadski revizor, „Rezultati – i osobito krajnji učinci – prikupljanja obavještajnih podataka te njihove procjene i izvještavanje o njima, inherentno su teško mjerljivi.“[4] Ovo posebno važi za situaciju kada je predmet operacije događaj koji se nikad i ne dogodi, kao što je teroristički napad. Samo nadzorno tijelo sa dovoljno znanja i iskustva može na pravi način vrednovati neopipljive koristi od neke obavještajne operacije i utvrditi da li je ona donijela odgovarajuću vrijednost za uloženi novac.

2.4.3 Tajnost i zloupotreba javnih sredstava

Obavještajnim službama je, razumljivo, važno da osjetljive informacije, kao što su operativni detalji i identitet izvora, ostanu povjerljive. Prema tome, one te informacije razdvajaju na dijelove, čime ograničavaju znanje o njima na minimalan broj ljudi, čak i

među uposlenicima same službe. Međutim, što je manji krug onih koji su upoznati, to je veći rizik da će javna sredstva biti podložna zloupotrebi. Na primjer, ako su informacije o nekom doušniku ograničene na obavještajnog službenika koji „vodi" tog doušnika, tada postoji prilika da službenici stvaraju nepostojeće „fantomske agente" u cilju pronevjere sredstava koja se navodno isplaćuju tim agentima. Čak i kada su doušnici stvarni, pravila o tajnosti mogu olakšati obavještajnim službenicima mogućnost da zadrže za sebe novac raspodijeljen doušnicima, a da pri tome nema velikog rizika da će biti otkriveni.

2.4.4 Sukobi interesa

Obavještajni službenici ponekad, što predstavlja dio njihovog rada, tajno plaćaju ljude da im daju informacije ili izvrše usluge, kao što je korištenje kuće iz koje se provodi nadzor. Odluke o tome kome platiti i koliko platiti u velikoj mjeri su diskreciono pravo samog službenika i možda njegovog nadređenog. To stvara potencijalni sukob interesa zato što će se odluke službenika vjerovatno temeljiti ne samo na vrijednosti onog koji pruža uslugu već i na ličnim vezama, a pogotovo s obzirom na povjerljivu prirodu transakcije, na stepen povjerenja kojeg službenik ima u onog koji mu pruža tu uslugu. Kao rezultat, neki službenici mogu angažirati ljude samo za to što su njihovi poznanici. Službenici mogu također isplaćivati pretjerane svote novca zato što je onaj koji im pruža tu uslugu bliski saradnik. U nekim slučajevima, službenici mogu čak uzeti novac za sebe. (vidjeti Okvir 1).

Okvir 1: Slučaj Kylea Foggoa[5]

Kyle Foggo je nekada radio za CIA-u kao viši obavještajni službenik. Njegove odgovornosti uključivale su nabavku robe i ugovaranje usluga za vrlo osjetljive operacije, uključujući izgradnju tajnih pritvorskih jedinica u inostranstvu. Da bi nabavio materijal za neke od tih pritvorskih jedinica, Foggo je dogovorio da CIA sklopi ugovor sa kompanijom koja je bila povezana sa njegovim bliskim prijateljem. Tužioci su kasnije utvrdili da je Foggo sklopio više ugovora sa tom kompanijom plaćajući po "napuhanim" cijenama robu i usluge koje je pružala. Zauzvrat, Foggo je imao od toga koristi, uključujući skupa ljetovanja i obećanja budućeg zaposlenja. Skrivajući taj odnos od kolega, Foggo je nastojao opravdati angažiranje te kompanije tvrdnjom da mu je bilo potrebno da nabavi robu i ugovori usluge od pružaoca usluga u kojeg ima povjerenja, a da je također želio izbjeći standardnu birokratsku proceduru nabavki. Na kraju, Foggo je priznao krivicu u slučaju korupcije i odslužio zatvorsku kaznu.

2.4.5 Rizici povezani sa raspoloživom imovinom i prihodom

Obavještajne službe nabavljaju značajne količine sredstava kao dio svojih operacija. Na primjer, one kupuju skupa vozila ili koriste skupe hotele kako bi svom agentu omogućile da se poveže sa nekim bogatašem koji je predmet tajnog praćenja tokom neke operacije. Obavještajni službenici mogu nastojati izvući profit iz takve vrijedne robe onda kada im ona više ne treba tako što će je zadržati za ličnu upotrebu, prepustiti je poznanicima, ili je prodati a za sebe zadržati prihod od prodaje. Činjenica da su ta sredstva nabavljena tajno povećava rizik. Slično, neke obavještajne službe uspostavljaju tzv. „maskirna preduzeća" kako bi prikrili tajne aktivnosti. Neke od tih kompanija mogu stjecati prihod čime nastaje rizik da službenici nezakonito zadržavaju prihod za sebe. Zbog takvih rizika, tijela za nadzor moraju pratiti ne samo rashode obavještajne službe, već i sredstva i prihod od usluga koje oni koriste.

2.4.6 Korištenje obavještajnih službi u političke svrhe

Zloupotreba sredstava obavještajne službe može se proširiti na članove izvršne vlasti koji su odgovorni za obavještajne službe. Ti zvaničnici povremeno koriste sredstva službe u nezakonite političke svrhe koje podrazumijevaju trošenje javnih sredstava. Stoga, tijela za nadzor treba da usmjere pažnju na ponašanje ne samo službenika obavještajnih službi, već i njihove interakcije sa zvaničnicima izvršne vlasti.

3. BUDŽETI ZA OBAVJEŠTAJNI RAD

Budžet je dokument sa pojedinačnim stavkama koji sadrži detaljno planirane prihode i rashode za predstojeći vremenski period, obično za fiskalnu godinu. On je, stoga, ključno sredstvo za usmjeravanje i kontrolu rada javnih agencija, pošto su agencijama potrebna sredstva da bi funkcionirale. U demokratskim zemljama, budžet obično usvaja parlament kao zakonodavni akt.

U nekim zemljama, obavještajne službe su organizacijski autonomne i imaju vlastiti budžet. U drugim, opet, one djeluju unutar ministarstava – kao što je francusko Ministarstvo unutrašnjih poslova, čiji je dio francuska unutarnja obavještajna služba (La Direction Centrale du Renseignement Intérieur). U tom slučaju, obavještajna služba nema vlastiti budžet. Umjesto toga, ona se finansira u okviru budžeta ministarstva kojem pripada. Tako, pojam *budžet za obavještajni rad* može izazvati zabunu jer se nekad odnosi na budžet pojedinačne službe, a nekad na budžet više službi unutar jednog ministarstva. Taj izraz se također može odnositi na zbirne iznose za cijelu obavještajnu zajednicu u okviru nekoliko ministarstava.

Organizacijski status službe je važan zbog posledica na nadzor nad budžetom službe. Kao opće pravilo, oni koji provode vanjski nadzor mogu provesti direktniju, detaljnu provjeru finansija obavještajnih službi koje su uspostavljene kao autonomne agencije, nego što je to slučaj sa finansijama obavještajnih službi koje djeluju unutar nekog ministarstva. To je stoga što finansije autonomne službe nisu povezane sa onima drugih odjela ministarstva.

Budžet vladinih agencija, bilo da su to agencije koje obavljaju obavještajni rad ili ne, treba da bude „sveobuhvatan“. Svjetska banka koristi ovaj termin u smislu da budžet „mora obuhvatati sve fiskalne operacije”.[6] Drugim riječima, budžet jedne vladine agencije treba uključiti sve finansijske aktivnosti koje se odnose na tu agenciju.[7] Osobito obavještajne službe treba da poštuju ovaj zahtjev zato što su neke u prošlosti prikupljale novac i trošile ga na aktivnosti koje zakonom nisu odobrene. Jedan takav primjer bi bio korištenje prihoda koji je CIA prikupila od iranskog oružja za finansiranje podrške nikaragvanskim *kontrašima* sredinom 1980-ih godina.

3.1 BUDŽETSKI CIKLUS

Termin budžetski ciklus odnosi se na cijeli proces kojim se novac traži, raspodjeljuje i troši, uključujući i naknadnu ocjenu te potrošnje. Postoje četiri glavne faze u budžetskom ciklusu:

- formuliranje, tokom kojeg nadležna ministarstva, vladini odjeli i agencije utvrđuju planirane prihode i potrošnju;
- provjera i odobravanje, tokom kojeg parlament dopunjava i mijenja te usvaja budžet;

- provedba, tokom koje agencija provodi plan razrađen detaljno u budžetu;
- naknadna provjera, tokom koje tijela za nadzor ocjenjuju korištenje novca od strane agencije; iza ovoga može slijediti parlamentarno glasanje o završnom računu budžeta za datu godinu.[8]

Mada se budžet obavještajnih službi formulira u velikoj mjeri na isti način kao i budžeti drugih vladinih odjela i agencija, drugačije su procedure njegove provjere, odobravanja, provedbe, kao i naknadne ocjene (razmatrane u Dijelovima 5 – 6 ovog dokumenta).

3.2 PRISTUPI IZRADI BUDŽETA

Tradicionalno, pri izradi budžeta koristi se metod „linija-stavka", pri čemu se raspodjeljuju određeni iznosi (eng. inputs) kako bi se pokrili projicirani troškovi, a da se pri tome troškovi ne vezuju za ciljeve politika. Nasuprot ovom linijskom budžetu, mnoge zemlje (kao što je Francuska) danas koriste metod izrade budžeta na osnovu „učinka" ili „rezultata" koji povezuje raspodjelu sredstava sa ciljevima politika i, u konačnici, sa željenim ishodima (tzv. programski budžet).[9] Pristup izradi budžeta ima važne implikacije za naknadni nadzor. Kako programski budžet uspostavlja veze između troškova i rezultata, lakše je naknadno procjenjivati provedbu budžeta, uključujući i faktore poput djelotvornosti i dobijene vrijednosti za uložen novac. Nasuprot tome, linijski budžet ne daje okvir za ocjenu provedbe budžeta.

3.3 OBJAVLJIVANJE BUDŽETA ZA OBAVJEŠTAJNI RAD

Koliko je poznato, nema vlade koja javnosti u potpunosti podnosi izvještaj o budžetu svojih obavještajnih službi. U većini slučajeva, detalji o budžetu se ne otkrivaju, i to ne samo javnosti, već ni članovima parlamenta koji ne pripadaju nadzornom odboru ovlaštenom da dobija klasificirane informacije u ovom domenu.

Tajnovitost koja okružuje budžet za obavještajni rad motivirana je brigom obavještajne službe da bi objavljivanje informacija o budžetu koristilo njihovim neprijateljima. To je, međutim, vjerovatno tačno samo ako objavljene informacije sadrže detalje koji su vezani za određene ciljeve, metode ili izvore informacija. U većini slučajeva, može se otkriti mnogo više informacija nego što je sada slučaj a da se pritom ne izlaže riziku državna sigurnost, već se time samo značajno povećava transparentnost.

Općenito govoreći, demokratske zemlje biraju između tri pristupa javnom objavljivanju budžeta za obavještajni rad. Neke (poput Ujedinjenog Kraljevstva[10]) objavljuju samo ukupni iznos raspodjeljen cjelokupnoj državnoj obavještajnoj zajednici zemlje. Drugi (poput Njemačke) objavljuju pojedinačni ukupni iznos za svaku obavještajnu službu. Očito, nijedan od ova dva pristupa ne otkriva nikakvu vezu između dodijeljenih sredstava i specifičnih ciljeva politika – što su informacije koje bi mogle biti korisne za vođenje javne debate koja se zasniva na dobroj obaviještenosti učesnika. Treći pristup (primjenjuju ga, na primjer, Australija i Francuska) je objavljivanje konkretnih iznosa raspodijeljenih u određene svrhe. Na primjer, u Francuskoj se javnosti predočava godišnji budžet za vanjsku obavještajnu službu (Direction Générale de la Securité Exterieure - DGSE), pri čemu se zasebno navodi i spisak odobrenih rashoda za osoblje, operativne troškove i investicije, kao i ukupni iznos određen za specijalne operativne aktivnosti (fr. *les fonds spéciaux*).

Vlade koje utvrđuju budžet na osnovu učinka (Australija i Francuska) mogu također objaviti ciljeve politika i željene rezultate tako da javnost sama može sagledati tu vezu. Javna verzija budžeta DGSE-a za 2010. godinu, na primjer, navodi „poboljšanje kapaciteta DGSE-a u prikupljanju i analizi obavještajnih informacija" kao ključni cilj politike, pri čemu se navodi planirano zapošljavanje 690 dodatnih uposlenika između 2009. i 2015. godine kao sredstvo za postizanje tog cilja.[12]

Objavljivanje što je moguće više informacija o budžetu – što treći pristup postiže bolje od ova dva – korisno je za društvo iz nekoliko razloga. Prvo, time se poštuje pravo javnosti da zna kako se javna sredstva troše. Drugo, pojačava transparentnost – čime omogućava parlamentarcima, medijima a čak i ostalim pripadnicima javnosti da učestvuju na pravi način u javnoj debati o finansiranju, politikama i prioritetima obavještajnih službi. Ozbiljna javna rasprava tjera vlade da pravdaju svoje prioritete u potrošnji, što u krajnjoj instanci promovira efikasnije korištenje javnih sredstava. Konačno, otvorena debata jača povjerenje javnosti u obavještajne službe, čime se ruše mitovi o tome koje su svrhe potrošnje za obavještajni rad te povremeno čak za rezultat ima i povećanje sredstava za obavještajne službe.

Odluka o količini informacija o budžetu koju treba objaviti ne smije se prepustiti isključivo izvršnoj vlasti. Parlamenti trebaju zakonski regulirati koje finansijske informacije mogu ostati tajna a koje se moraju objaviti. Bez obzira na to koliko se informacija o budžetu objavi, bitno je da parlamentarni odbori koji su uključeni u kontrolu, te koji mijenjaju i/ili odobravaju budžet za obavještajne službe, imaju pristup svim relevantnim informacijama, uključujući klasificirane dijelove budžeta (Vidjeti Dio 5.1).[13]

4. MEHANIZMI UNUTARNJE FINANSIJSKE KONTROLE I REVIZIJE

Mada je ovo poglavlje usmjereno na ulogu koju vanjska tijela za nadzor imaju u praćenju finansija obavještajnih službi, njena prezentacija bi bila nepotpuna bez rasprave o internim finansijskim kontrolama koje postoje unutar obavještajnih službi. Bez takvih mehanizama, vanjski nadzor bio bi mnogo manje učinkovit.

4.1 RAČUNOVODSTVO

Uobičajeni važeći zakoni zahtijevaju od svih javnih agencija, uključujući obavještajne službe, da odrede službenika zaduženog za računovodstvo – čija odgovornost je da osigura da agencija vodi urednu i preciznu finansijsku evidenciju usklađenu sa svim primjenjivim propisima (vidjeti Okvir 2). Često je službenik odgovoran za računovodstvo istovremeno i direktor agencije koji u toj ulozi ima podršku finansijskog odjela koji obavlja svakodnevni rad na vođenju evidencije i izvještavanju o svim finansijskim transakcijama agencije. Finansijski odjel također uspostavlja i provodi finansijske kontrole kako bi osigurao da se sredstva propisno koriste.

Okvir 2: Južnoafrički Zakon o računovodstvenim službenicima

Ovaj okvir predstavlja sažete, odabrane odredbe Zakona o upravljanju javnim finansijama Južne Afrike iz 1999. godine, kojim se reguliraju unutarnje finansijske kontrole za vladine agencije (uključujući obavještajne službe). U skladu sa ovim Zakonom, računovodstveni službenici u Južnoj Africi imaju široku odgovornost da osiguraju da njihove agencije provode dobre finansijske prakse.

Svaka agencija južnoafričke vlade mora imati službenika zaduženog za računovodstvo koji je odgovoran za:

1. osiguravanje da agencija sačuva učinkovit, efikasan i transparentan sistem upravljanja finansijskim rizikom, kao i interni sistem revizije pod kontrolom odbora za reviziju koji djeluje u skladu sa primjenjivim propisima;
2. učinkovito, efikasno, ekonomično i transparentno korištenje sredstava agencije;
3. upravljanje aktivom i pasivom agencije, uključujući čuvanje sredstava agencije;
4. osiguravanje da rashodi agencije budu u skladu sa relevantnim zakonima o budžetu.

Zakon dalje zadužuje službenike zadužene za računovodstvo da sprječavaju i, ako je to potrebno, odgovaraju na neodobrenu, nepravilnu ili rastrošnu potrošnju agencije. Kada se takva potrošnja otkrije, službenik zadužen za računovodstvo mora odmah o tome podnijeti pismeni izvještaj trezoru koji sadrži pojedinosti potrošnje i, u slučaju neregularne potrošnje u koju je uključena i nabavka robe ili ugovaranje usluga, nadležnom odboru za tender. Usto, službenik zadužen za računovodstvo mora preduzeti odgovarajuće disciplinske mjere protiv bilo kojeg zvaničnika koji podriva sistem finansijskog upravljanja agencije, ili koji čini (ili dopušta da se čine) neovlaštenu, nepravilnu ili rastrošnu potrošnju.

U pogledu vođenja evidencije, službenik zadužen za računovodstvo mora čuvati potpunu i propisnu evidenciju o finansijskom poslovanju agencije, u skladu sa propisanim normama i standardima

Propisno interno računovodstvo je od suštinskog značaja za rad vanjskih tijela za nadzor zato što bi bez toga glavne revizorske institucije i druga takva tijela imala velikih poteškoća u rekonstruiranju transakcija i uz njih povezanih aktivnosti. Općenito govoreći, kvalitet računovodstva obavještajnih službi pokazuje da li je njihova finansijska evidencija ispravna i da li odgovara istini.

4.2 SMJERNICE ZA FINANSIJSKI MENADŽMENT

Kao i sve vladine agencije, i obavještajne službe formaliziraju svoj finansijski menadžment i računovodstvene procedure kroz paket pisanih smjernica. Obično ih daje direktor službe, ili izvršni direktor, a onda ih procjenjuje vanjsko tijelo za nadzor, te ove smjernice predstavljaju dio regulatornog okvira u odnosu na kojeg se ocjenjuje rad pripadnika službe.

Smjernice za finansijski menadžment obuhvataju obično sljedeća pitanja:

- Ko odobrava ostvarenje prihoda i rashoda i koji se proces pri tome primjenjuje? Odgovarajući na ovo pitanje, smjernice treba da utvrde jasne linije odgovornosti i podnošenje računa za finansijske transakcije.
- Koje je dopušteno korištenje sredstava službe? Odgovor na ovo pitanje treba da bude usklađen sa relevantnim zakonima.
- Kako finansijske transakcije treba da se odvijaju? Smjernice treba da daju savjet,

recimo, o tome da li operativci treba da koriste gotovinu ili da vrše elektronsko plaćanje.

- Koje finansijske evidencije treba čuvati? Propisno vođenje evidencije je važno zato što se time uspostavlja trag za reviziju za kasniju upotrebu. Međutim, u nekim zemljama, poput Sjedinjenih Država, zakon koji ovo određuje dopušta obavještajnim službama da koriste "lažne račune"u vezi sa nekim osjetljivim operacijama (npr. strane obavještajne operacije). Smjernice za te račune obično dopuštaju trošenje samo izvršnog službenika i ne trebaju se potkrepljivati cijelim setom računa.[14]

4.3 FINANSIJSKO IZVJEŠTAVANJE

Zakon koji regulira ovo pitanje obično zahtijeva da sve javne agencije, uključujući obavještajne službe, pripremaju detaljne godišnje izvještaje o svojim finansijskim transakcijama.[15] Bez takvih izvještaja, vanjska tijela za nadzor ne mogu provesti reviziju finansija i aktivnosti službe.

Obavještajne službe obično dostavljaju te izvještaje izvršnoj vlasti, glavnoj revizorskoj instituciji i parlamentu. Kao i kod budžeta za obavještajni rad, međutim, ti izvještaji razlikuju se u pogledu količine detalja koje sadrže.

Kao što izvršna vlast ne treba da ima ovlast da jednostrano utvrđuje koje informacije o budžetu treba otkriti a koje se mogu zadržati, također ne treba da ima ovlast da sama utvrđuje koje informacije su pogodne za uključivanje u finansijske izvještaje, a koje mogu ostati tajne. Umjesto toga, parlament treba zakonima da utvrdi detaljne kriterije za reguliranje finansijskih informacija koje trebaju biti stavljene na uvid javnosti i onih koje mogu ostati povjerljive (vidjeti Okvir 3).

Okvir 3: Finansijsko izvještavanje prema zakonima Novog Zelanda

Ovaj okvir daje sažete, odabrane odredbe Zakona o javnim finansijama iz 1984. godine, te Zakona o sigurnosno-obavještajnoj službi iz 1969, koji zajedno reguliraju način na koji obavještajne službe Novog Zelanda pripremaju finansijske izvještaje. On pravi usporedbu između zahtjeva koji se postavljaju pred obavještajne službe sa onima koje treba da ispunjavaju druge javne agencije.

Što je moguće prije nakon završetka svake fiskalne godine, javne agencije na Novom Zelandu moraju pripremiti finansijske izvještaje koji obuhvataju prethodnu fiskalnu godinu i dostaviti ih nadležnom ministru. Ti izvještaji moraju uključiti potpune finansijske podatke kao i informacije o operacijama agencije te izjavu o njenom radu. Općenito govoreći, ti izvještaji moraju pružiti dovoljno informacija kako bi se omogućila ocjena koja se temelji na potpunoj informiranosti o radu agencije tokom prethodne fiskalne godine – posebno u pogledu ciljeva, pokazatelja i standarda utvrđenih za agenciju na početku godine.

Što se tiče većine javnih tijela, zakon zahtijeva da nadležni ministar kada dobije izvještaj dostavi taj izvještaj parlamentu i da ga objavi što je moguće prije. Za izvještaje obavještajnih službi, međutim, rješenja se razlikuju. Umjesto dostavljanja potpunog izvještaja parlamentu u plenarnom sastavu, odgovorni ministar dostavlja ga samo Odboru za obavještajna i sigurnosna pitanja, čiji članovi imaju ovlaštenje da pregledaju klasificirane informacije. Za plenarni sastav parlamenta, ministar priprema pročišćenu verziju, koja mora uključiti izjavu o ukupnoj potrošnji. Tu redigiranu verziju izvještaja ministar kasnije podnosi javnosti.

Što se tiče budžeta za obavještajni rad, Australija i Francuska imaju dobre prakse u tom pogledu. Njihove obavještajne službe pripremaju relativno detaljne finansijske izvještaje za javnost. Javnosti dostupni izvještaji Australijske organizacije za sigurnost i obavještajni rad (ASIO) sadrže pojedinačne kategorije troškova kao što troškovi uposlenih, isporuke robe (uključujući robu i usluge), te troškove deprecijacije/amortizacije. Izvještaji također sadrže po kategorijama podijeljene troškove za prihode, kao što su vlastiti prihodi, prodaja imovine, te prihod vlade.[16] Francuski zakon zahtijeva da finansijski izvještaji obavještajnih službi uključe detaljne anekse za svaku misiju službe. Ti aneksi moraju uključiti ne samo finansijske podatke, već i ocjenu političkih ciljeva i željenih ishoda koji se utvrđuju na početku budžetskog ciklusa.[17]

Iz istih gore navedenih razloga u vezi sa informacijama o budžetu, obavještajne službe treba da sačine javnu verziju svojih finansijskih izvještaja što je moguće detaljnije, a da pri tome ne ugroze povjerljivost svoga rada i ne izlože riziku državnu sigurnost.

5. PARLAMENTARNI NADZOR

Ovaj dio se bavi nadzornom ulogom koju igraju članovi parlamenta tokom finalne tri faze budžetskog ciklusa – provjera i odobravanje, provedba i naknadna ocjena. Mada rad obavještajnih službi uključuje osjetljiva pitanja, parlamenti treba da finansije obavještajne službe podvrgnu istom nivou nadzora kojoj su podvrgnute finansije drugih javnih agencija. Jedini ustupak koji se čini treba da bude korištenje zaobilaznijih mehanizama nadzora.

Parlamentarni nadzor nad obavještajnim službama neizbježno se u najvećoj mjeri odvija iza zatvorenih vrata. Ipak, i dalje je važno da parlamenti obavještavaju javnost o svom nadzornom radu kroz javne izvještaje i javna saslušanja (vidjeti Poglavlje 3 - Nathan). Transparentnost promovira povjerenje javnosti ne samo u parlamentarni nadzor, već i u rad obavještajnih službi.

5.1 PROVJERA I ODOBRAVANJE BUDŽETA

U većini demokratskih zemalja, parlamenti provjeravaju, dopunjuju i mijenjaju, te odobravaju budžete agencije koje predlaže izvršna vlast. Ne postoji valjan razlog zašto budžeti obavještajnih službi treba da budu isključeni iz tog procesa.

Kako bi se zaštitile klasificirane informacije, parlamenti mogu uspostaviti posebne mehanizme kontrole klasificiranih segmenata budžeta. Međutim, bez obzira na to koji mehanizmi se koriste, u plenarnom sastavu parlament treba uvijek da glasa o sredstvima obavještajne službe kao dio procesa davanja odobrenja za budžet vlade. Glasanje u plenarnom sastavu treba da ide uz, a ne da bude zamjena punog i detaljnog nadzora odbora za budžet, odbora za nadzor nad obavještajnim službama ili specijalnog povjerljivog odbora.[18]

5.1.1 Odbori za budžet

Neki parlamenti koriste redovne odbore za budžet (ili sredstva) kako bi kontrolirali finansije obavještajnih službi. Ti odbori mogu odrediti članove, poznate kao izvjestioce, da preuzmu odgovornost za određenu službu, ministarstvo ili misiju. Ti izvjestioci obično sačinjavaju izvještaje u kojima su sadržane preporuke na osnovu kojih odbor u punom sastavu vodi

diskusiju, dopunjuje i mijenja, i odobrava budžete službi.

Odbori za budžet su po mnogo čemu dobro izabrano mjesto za ocjenu zahtjeva obavještajne službe u širem kontekstu cijelog budžeta za izvršnu vlast. Ali u odsustvu specijaliziranih izvjestilaca, članovi odbora vjerovatno neće imati potrebno vrijeme niti specifično stručno znanje da bi na propisan način proveli nadzor nad obavještajnim službama. Odbori za budžet također pokazuju tendenciju nedostatka dovoljnog pristupa klasificiranim informacijama, što dalje ograničava njihovu sposobnost da kontroliraju budžete službi.

5.1.2 Odbori za nadzor nad obavještajnim službama

Odbori za nadzor nad obavještajnim službama (vidjeti Poglavlje 2 - Farson, i Poglavlje 3 - Nathan) obično imaju pristup klasificiranim informacijama koje nisu dostupne drugim članovima parlamenta. Oni obično usmjeravaju pažnju na naknadnu ocjenu, uključujući revizije finansija službe. U nekim zemljama, međutim, njihova odgovornost je proširena na kontrolu budžeta i njegovo odobravanje. U Mađarskoj, parlamentarni Odbor za državnu sigurnost razmatra i daje mišljenje o onim dijelovima budžeta za obavještajnu službu koji su klasificirani te prema tome nisu dostupni parlamentu u plenarnom sastavu.[19] Kongres SAD ima kompleksniji proces koji je opisan u Okviru 4. U drugim zemljama, (npr. u Njemačkoj, vidjeti Okvir 5) odbori za nadzor nad obavještajnim službama igraju sekundarnu ulogu, jer daju savjete drugim odborima (poput odbora za budžet ili sredstva) koji imaju primarnu odgovornost za kontrolu budžeta.

Odbori za nadzor nad obavještajnim službama su prava tijela za procjenjivanje i razumijevanje budžeta obavještajnih službi zato što su upoznati sa aktivnostima, procedurama i politikama tih službi. Ipak, učinkovitost takve jedne kontrole zavisi od nekoliko faktora:

- resursa odbora, istražnih ovlasti, te pristupa klasificiranim informacijama (vidjeti Poglavlje 2 i 3);
- stepena do kojeg članovi odbora imaju vremena, osoblja i stručnog znanja da izvršavaju svoje zadatke;
- volje članova odbora da ispunjavaju svoje zadatke;
- sposobnost odbora da utječe na budžetski proces (posebno kada je njegova uloga savjetodavna).

U pravim okolnostima, odbor za nadzor nad obavještajnim službama sa značajnim budžetskim odgovornostima može koristiti svoju ovlast da daje odobrenje kako bi osigurao da predloženi budžet uzme u obzir prethodne preporuke odbora o načinu poboljšanja učinkovitosti, efikasnosti i poštivanja zakona date službe.

Okvir 4: Kongresna kontrola i odobravanje budžeta američkih obavještajnih službi[20]

Proces kojim Američki kongres kontrolira i odobrava budžete za obavještajne službe uključuje ne manje od osam odbora i pododbora. On ima dva bitna aspekta: davanje saglasnosti i raspodjelu sredstava.

Davanje saglasnosti

Odluka o davanju saglasnosti Kongresa, kada je potpiše predsjednik, regulira aktivnosti vladinih agencija, uključujući i njihove budžete. Za budžete obavještajnih službi, proces davanja saglasnosti počinje sa prijedlogom koji izvršna vlast dostavi Kongresu. Ti prijedlozi se onda razmatraju u Predstavničkom domu u Stalnom odboru za obavještajna pitanja i Odboru za oružane snage, a u Senatu u Stalnom odboru za obavještajna pitanja te Odboru za oružane snage. Ovi odbori mogu preusmjeriti određene iznose u okviru budžeta. Oni, također, mogu zabraniti određene aktivnosti i uključiti nove inicijative. Kada odbori parlamentarnih domova dovrše zakon o davanju saglasnosti, o njemu se glasa u plenarnom sastavu. Kada Predstavnički dom i Senat odobre zakon o davanju saglasnosti, ti zakoni se usaglase te ponovo dobiju saglasnost u oba Doma i onda šalju predsjedniku na potpisivanje.

Svaka odluka o davanju saglasnosti za obavještajnu službu ima klasificiran aneks koji sadrži listu po kategorijama aktivnosti za koje je svaka služba ovlaštena da primi određeni iznos te svrhu za koju su namijenjena ta sredstva. Na taj način, odluke o davanju saglasnosti (kada se unesu u zakon) utvrđuju parametre za potrošnju obavještajnih službi. Međutim, odluke o davanju saglasnosti ne jamče da će odobreni programi zaista biti i finansirani. Konačne odluke o finansiranju donose se u toku procesa raspodjele sredstava.

Raspodjela sredstava

Odluka o dodjeli sredstava je slična zakonu o budžetu u drugim zemljama - to je pravni instrument kojim se trezorska sredstva raspodjeljuju za agenciju ili program. Odbori za budžet Kongresa i Senata imaju pododbore za odbranu u čijoj je nadležnosti gotovo cjelokupna američka obavještajna zajednica. Na osnovu prijedloga dobivenih od izvršne vlasti, ti pododbori izrađuju nacrt zakona o budžetu za obavještajne službe.

Mada zakon o budžetu mora biti generalno usklađen sa postojećim zakonu o davanju saglasnosti, oni mogu povećati ili smanjiti sredstva za specifične obavještajne programe. Ako ne postoji takav zakon o davanju saglasnosti, zakoni o budžetu mogu uključiti blanko saglasnosti za sve obavještajne aktivnosti.

Kao i u slučaju odluke o odobrenju, zakon o budžetu mora proći složen proces odobravanja. On mora biti odobren u pododborima, a onda u odborima u punom sastavu, i potom u plenarnom sastavu oba Doma – nakon čega mora biti usaglašen i ponovo odobren od strane oba Doma, te na kraju poslan predsjedniku SAD-a na potpisivanje.

5.1.3 Specijalni povjerljivi odbori

Parlamenti ponekad koriste treći mehanizam, specijalni povjerljivi odbor, da kontroliraju budžet obavještajne službe. Dobar primjer ovog mehanizma je Povjerljivi odbor koji je uspostavljen u Njemačkom Bundestagu (vidjeti Okvir 5).

Okvir 5: Povjerljivi odbor njemačkog Bundestaga[21]

Bundestag, donji dom Njemačkog parlamenta, upućuje pitanja u vezi sa budžetom koja se odnose na tri savezne obavještajne službe posebno uspostavljenom Povjerljivom odboru. Ovaj Odbor obavlja iste funkcije kao i Odbor za budžet i Odbor za javnu reviziju Bundestaga prema drugim javnim odjelima i agencijama. To znači da on nadzire budžet koje predloži izvršna vlast, daje preporuke za njegovo poboljšanje, te prati njegovu provedbu.

Izbor članova odbora

Povjerljivi odbor ima deset članova čija se mjesta dodjeljuju proporcionalno političkim partijama, u skladu sa njihovom zastupljenošću u Bundestagu. Imenovani članovi Odbora ne prolaze posebnu sigurnosnu provjeru, ali moraju osigurati većinu, poznatu kao „kancelarova većina“, tj. većina članova Bundestaga mora glasati za njih, što pokazuje da imaju povjerenje parlamenta.

Nadzor i odobrenje budžeta za obavještajne službe

Kontrola od strane odbora i odobrenje budžeta za obavještajnu službu ide ovim tokom:

1. izvršna vlast dostavlja odboru detaljni budžet za svaku obavještajnu službu;
2. Odbor se sastaje sa zvaničnicima ministarstva i višim rukovodstvom službe kako bi razmotrili predložene budžete;
3. Odbor se konsultira sa Odborom za nadzor nad obavještajnim službama Bundestaga;
4. Odbor dopunjava i mijenja budžet, ako smatra potrebnim, prije nego što ga vrati izvršnoj vlasti koja mora prihvatiti te promjene;
5. Predsjedavajući odbora prenosi Odboru za budžet ukupne iznose raspodijeljene svakoj službi. Odbor za budžet onda unosi te brojke (bez debate) u svoje preporuke o budžetu;
6. Parlament u plenarnom sastavu glasa o cjelokupnom budžetu vlade.

Istražne ovlasti i pristup informacijama

Važeći zakon daje Povjerljivom odboru veliku istražnu ovlast i širok pristup klasificiranim informacijama, uključujući sposobnost da pregleda sve dosjee i dokumente pod kontrolom obavještajne službe, te da izvrši inspekciju svih prostorija službe. Usto, Odbor može zatražiti od zvaničnika službe i predstavnika izvršne vlasti da odgovaraju na pitanja, koristeći pomoć vanjskih eksperata, ukoliko je to potrebno.

5.2 PRAĆENJE PROVEDBE BUDŽETA

Kada se odobre budžeti javnih agencija, parlamenti imaju odgovornost da prate potrošnju agencije kako bi osigurali da se budžeti propisno provode. U pogledu obavještajnih službi, to praćenje obično vrši odbor parlamenta zadužen za nadzor nad obavještajnim službama (ili posebni povjerljivi odbor), čiji članovi imaju privilegiran pristup klasificiranim informacijama. U praksi, međutim, odbori za nadzor nad obavještajnim službama imaju tendenciju da zahtijevaju da im se dostave finansijske informacije samo ako se pojave navodi o nepropisnom radu u vezi sa određenim programom ili aktivnošću zato jer većina parlamentaraca nema ni vremena niti sredstava da detaljno razmotri ogromnu količinu finansijskih informacija, osim možda kada se utvrđuju budžeti.

S obzirom na ova ograničenja, praćenje provedbe koje obavlja parlament obično je ograničeno na informacije koje se proaktivno daju (to jest, da ne budu tražene) od izvršne

vlasti i obavještajnih službi. Stoga, važeći zakon u mnogim demokratskim zemljama zahtijeva od izvršne vlasti i/ili obavještajnih službi da otkrivaju informacije o finansijama službe na periodičnoj osnovi.[22] U Italiji, na primjer, od premijera se traži da svakih šest mjeseci parlamentarnom Republičkom odboru za sigurnost (COPASIR) podnosi izvještaj o provedbi budžeta obavještajnih službi.[23]

Parlamenti također moraju razmotriti zahtjeve za dodatno finansiranje koji se pojave u toku fiskalne godine. U slučaju obavještajnih službi, ti zahtjevi se mogu odnositi na nepredviđene događaje, kao što su teroristički napadi. Kao i sa drugim pitanjima koja su vezana za provedbu, razmatranja ovih zahtjeva obično se delegiraju odboru parlamenta za nadzor nad obavještajnim službama. U Španiji, na primjer, zahtjevi za dodatno finansiranje se razmatraju u Odboru za tajne fondove, čije mišljenje se onda prenosi Parlamentu u plenarnom sastavu radi glasanja.[24]

5.3 NAKNADNA OCJENA

Naknadna ocjena finansija javnih agencija je prvenstveno odgovornost unutarnjih mehanizama revizije svake agencije (vidjeti Dio 4), te Glavne državne revizorske institucije (vidjeti Dio 6). Ipak, parlamenti igraju određenu ulogu u tom procesu, jer prate rad revizora i provode nezavisne istrage.

5.3.1 Parlamentarni mehanizmi za naknadnu ocjenu

Odbori za javnu reviziju (OJR), koji provode naknadnu provjeru finansija javnih tijela obično nisu odgovorni za ocjenu finansija obavještajnih službi zbog njihove osjetljive prirode. Umjesto toga, mnogi parlamenti imaju posebna rješenja za reviziju finansija obavještajne službe. U Ujedinjenom Kraljevstvu, na primjer, izvještaji i mišljenja Državnog ureda za reviziju (glavna revizorska institucija u Ujedinjenom Kraljevstvu) o obavještajnim službama se dostavljaju samo predsjedavajućem Odbora za javne račune.[25] Prvenstvena odgovornost za njihovu reviziju je umjesto toga na Odboru za obavještajne službe i sigurnost, čiji nadzorni mandat uključuje naknadnu ocjenu finansija obavještajnih službi (vidjeti Okvir 6). Drugdje, npr. u Njemačkoj (vidjeti Okvir 5), parlamenti su odredili odbor za obavljanje zadataka u ime parlamenta u pogledu budžeta i računa koji sadrže klasificirane informacije.

Okvir 6: Uloga Odbora Ujedinjenog Kraljevstva za obavještajne službe i sigurnost u *ex post* reviziji

Odbor Ujedinjenog Kraljevstva za obavještajne službe i sigurnost (ISC) uključuje članove iz oba doma parlamenta. Njegov mandat je nadzor nad „politikom, upravljanjem i potrošnjom“ obavještajnih i sigurnosnih službi.[26]

U skladu sa tim mandatom, ISC provodi naknadnu ocjenu finansija službe, prvenstveno na osnovu godišnjih mišljenja revizije i izvještaja koje pripremi Nacionalni ured za reviziju (NAO). Kao dio tog procesa, ISC drži saslušanja sa predstavnicima NAO i višim rukovodstvom službi kako bi razmotrio reviziju koju uradi NAO.

U vlastitom godišnjem izvještaju, ISC uključuje i procjenu finansija službe.[27] ISC prvo dostavlja svoj izvještaj premijeru, ali se on kasnije podnosi i javnosti.[28] Usto, ISC angažira i vlastitog istražitelja koji može biti angažiran u bilo kojem trenutku da razmotri, između ostalog, aspekte aktivnosti službe sa važnim finansijskim implikacijama.[29]

5.3.2 Proces i svrha naknadne ocjene

Parlamentarna naknadna ocjena finansija obavještajne službe obično je usmjerena na izvještaje GRI-ja. Parlamentarci odgovorni za ovu ocjenu također razmatraju godišnje i finansijske izvještaje koje pripremaju obavještajne službe.[30] Saslušanja tokom kojih revizori GRI-ja, zvaničnici izvršne vlasti i rukovodstvo obavještajne službe svjedoče su važan dio ovog procesa.

Prvenstvena svrha naknadne ocjene je utvrditi da li obavještajne službe:[31]

- izvršavaju svoj budžet onako kako je parlament odobrio na početku budžetskog ciklusa;
- troše i odgovaraju za javna sredstva u skladu sa primjenjivim zakonima i politikama;
- rade učinkovito i efikasno; i
- postižu programske ciljeve utvrđene na početku budžetskog ciklusa (ako se koristi pristup budžetu na osnovu učinka – tzv. programski budžet).

Prilikom zaključenja procesa revizije, parlamentarci koji provode reviziju mogu dati izvještaj koji sadrži preporuke za poboljšanje finansijskih praksi službi te mehanizme kontrole. U zemljama gdje važeći zakon zahtijeva da parlament u punom sastavu usvoji provedbu budžeta, takvi izvještaji mogu utjecati na glasanje u plenarnom sastavu.

Naknadna ocjena omogućava parlamentu da na ispravan način odobrava buduće budžete. Doista, parlamentarci mogu da koriste i svoje pravo prethodne provjere (*ex ante*) i da tako natjeraju izvršnu vlast i obavještajne službe da prihvate preporuke koje su rezultat naknadnog nadzora. Ovo sredstvo pritiska najbolje djeluje kada postoji jaka veza između prethodnog odobravanja budžeta i naknadne provjere njihove provedbe. To se može najbolje postići tako što će jedan parlamentarni odbor biti odgovoran za obje funkcije u vezi sa obavještajnim službama (kao što je to slučaj u Njemačkoj, vidjeti Okvir 5). Alternativno, koordinacija se može ojačati putem zajedničkih sastanaka i drugih oblika razmjena informacija između odbora i drugih tijela nadležnih za prethodni i naknadni nadzor.

5.3.3 Zahtijev za izvještajem glavnih revizorskih tijela

U nekim zemljama (kao što su Francuska i Sjedinjene Države), parlament može dati uputstvo glavnoj revizorskoj agenciji da istraži određeni program ili rashod, te da procijeni isplativost određene investicije.[32] Ovlaštenje dato parlamentu na ovaj način može pomoći da se osigura da rad glavnog ureda za reviziju podržava rad parlamentarnih nadzornih odbora. S druge strane, to može također preopteretiti glavni ured za reviziju te ispolitizirati njegov rad (ako, na primjer, utjecajni parlamentarci daju uputu glavnom uredu za reviziju da istraži pitanje iz političkih, odnosno partijskih razloga). U Francuskoj, stoga, važeći zakon ograničava broj zahtjeva koje parlament može dati i ostavlja otvorenu mogućnost da revizorski sud može odbaciti jedan ili više takvih zahtjeva. Slično, njemački zakon dozvoljava parlamentu da zahtijeva istragu Saveznog revizorskog suda (FCA), ali odriče parlamentu ovlast da osporava istrage koje provede FCA, čime se čuva nezavisnost FCA.[33]

6. GLAVNE REVIZORSKE INSTITUCIJE

U svakoj demokratskoj zemlji postoji neki oblik autonomne glavne revizorske institucije

odgovorne za reviziju javnih agencija, uključujući obavještajne službe. Mada su ove institucije usmjerene prvenstveno na finansijske aspekte rada vlade, njihova revizija se može proširiti na druge aspekte rada vladinih službi. Sveobuhvatna rasprava o raznim tipovima glavnih institucija za reviziju je izvan opsega ove ovog poglavlja, ali se može ukratko reći da glavne agencije za reviziju potpadaju pod dvije široke kategorije: model „suda“ (kao što je francuski Sud za reviziju) i model „ureda“ (kao što su Nacionalni ured za reviziju u Ujedinjenom Kraljevstvu i Ured za odgovornost vlade Sjedinjenih Američkih Država). Bez obzira na njihov specifičan oblik, glavne agencije za reviziju obično su glavna vanjska tijela odgovorna za naknadnu ocjenu finansija obavještajnih službi. Ono što je navedeno u ovom dijelu odnosi se na oba tipa glavnih institucija za reviziju.

6.1 NEZAVISNOST

Kako bi glavne revizorske institucije učinkovito obavljale svoje funkcije, one moraju biti oslobođene kontrole izvršne vlasti. Zapravo, Generalna skupština UN-a je usvojila rezoluciju u kojoj se priznaje značaj nezavisnosti glavnih institucija za reviziju.[34] Glavne revizorske institucije treba da imaju:

- *organizacijsku nezavisnost* - glavne revizorske institucije treba da budu uspostavljene zakonom kao autonomne institucije sa vlastitim budžetom.
- *operativnu nezavisnost* - glavne revizorske institucije trebaju biti slobodne da utvrđuju šta će biti predmet njihove revizije, kao i kako i kada će se ona vršiti kao, te koje će nalaze i preporuke dobiti u tim revizijama. Rad revizora mora biti zaštićen od miješanja bilo kojeg drugog tijela.
- *ličnu nezavisnost* - pojam lična nezavisnost odnosi se na poziciju samih revizora. Viši zvaničnici glavnih institucija za reviziju treba da budu izabrani kroz transparentan, inkluzivan i na zaslugama zasnovan proces koji zahtijeva od kandidata da dobiju podršku i parlamenta i izvršne vlasti. Kada su jednom imenovani, međutim, revizori treba da imaju nezavisnost zajamčenu zakonom kroz utvrđene mandate i druge mjere koje ih štite od odmazde ukoliko se njihovi nalazi pokažu nepovoljnim za aktualnu izvršnu vlast. Nasuprot tome, viši revizori treba da izbjegavaju političke ili poslovne aktivnosti koje bi mogle kompromitirati njihovu nezavisnost i/ili se smatrati sukobom interesa.

6.2 FUNKCIJE

Primarne funkcije glavne revizorske institucije su:

- razotkrivanje kršenja zakonitosti, efikasnosti, učinkovitosti i ekonomičnosti u finansijskom menadžmentu, kao i drugih odstupanja od prihvaćenih standarda;
- davanje preporuka za poboljšanje finansijskog upravljanja – uključujući unutarnje kontrole, upravljanje rizikom te sisteme računovodstva;
- osiguravanje parlamentu tačnih i redovnih vladinih računa čime se pomaže da se osigura da izvršna vlast ispunjava volju parlamenta;
- osiguravanje da javnost zna da li se njen novac zakonito, propisno, djelotvorno i učinkovito troši;
- osiguravanje odgovornosti javnih agencija za korištenje javnih sredstava.

Dok su mnoge od ovih funkcija po svojoj prirodi ex post funkcije– odnosno, podrazumijevaju ocjenu finansijskih aktivnosti nakon što su one obavljene – glavne revizorske institucije

mogu također igrati i ulogu prethodne, ex ante ocjene. Tako, jedna glavna revizorska institucija (poput Njemačkog saveznog suda za reviziju, vidjeti Okvir 9) može imati mandate da daje mišljenja o nacrtu budžeta.[35] To se može posmatrati kao preventivna funkcija sa ciljem utvrđivanja i ispravljanja finansijskih problema prije nego što se oni dese. Na primjer, revizorska institucija može preporučiti raspodjelu dodatnih sredstava za određenu aktivnost ili tip rashoda ako su njene prethodne revizije dosljedno utvrdile da se više sredstava trošilo na njih.

Glavne revizorske institucije nemaju mandat da tragaju za slučajevima prevara ili korupcije. Ali, ukoliko se otkriju dokazi o takvim praksama, glavne revizorske institucije treba da o njima izvijeste nadležne članove izvršne vlasti i/ili nadležne agencije za provedbu zakona.

6.3 ODNOSI SA OBAVJEŠTAJNIM SLUŽBAMA

Glavne revizorske institucije treba da provode reviziju obavještajnih službi korištenjem istih standarda koje primjenjuju u reviziji drugih javnih agencija te se, stoga, nadležnost glavne revizorske institucije treba da proširi na sve aspekte finansija obavještajne službe. Izvršnoj vlasti ne smije se dozvoliti da izuzima bilo koje područje obavještajne aktivnosti od vanjskog finansijskog nadzora zato što to podriva nezavisnost revizorske institucije, a i povećava rizik da nezakonito ili nepropisno korištenje novca može biti prikriveno.[36]

Neke zemlje (poput Francuske i Sjedinjenih Država) izuzimaju određene operativne račune obavještajnih službi iz obaveze da budu predmet revizije koju provodi glavna revizorska institucija. U tim slučajevima, dobra praksa zahtijeva da neko drugo nezavisno tijelo bude određeno da bi provodilo reviziju izuzetih računa. U Francuskoj, izuzeti računi su predmet revizije Odbora za posebne fondove, jedne hibridne grupe parlamentaraca i revizora.[37] U Sjedinjenim Državama, izuzeti računi mogu biti predmet revizije kongresnih odbora za nadzor nad obavještajnim službama.[38]

Bez obzira na to kako se obavlja revizija, sve finansijske aktivnosti obavještajne službe trebaju biti predmet revizije od strane tijela koje je vanjsko, kako prema obavještajnoj zajednici, tako i prema izvršnoj vlasti. Općenito govoreći, glavne revizorske institucije su u najboljoj poziciji da obavljaju tu reviziju.

6.4 TIPOVI REVIZIJE

Tipovi revizija koje obavljaju glavne revizorske institucije razlikuju se od zemlje do zemlje, ali sljedeća tri tipa su gotovo opšte prisutna:

- *finansijske revizije* - utvrđuju tačnost i ispravnost finansijskih izvještaja koje pripremaju javne agencije;.
- *revizije u pogledu poštivanja zakona* - utvrđuju da li su prihodi i rashodi jedne agencije u skladu sa važećim zakonima i propisima, uključujući zakon o godišnjem budžetu;
- *revizije učinka ili vrijednost-za-novac (VFM)* - utvrđuju da li su agencije bile učinkovite i efikasne u ispunjavanju svog mandata i ciljeva, to jest, da li su porezni obveznici dobili adekvat*nu vrijednost za javna sredstva koja su uložena u datu agenciju*.

U pogledu obavještajnih službi, glavne revizorske institucije prvenstveno provode finansijske revizije i revizije poštivanja zakona sa fokusom na unutarnje finansijske kontrole, upravljanje rizikom i sisteme računovodstva.

Pošto glavne revizorske institucije ne mogu provoditi reviziju svake pojedinačne finansijske transakcije koju izvrši određena agencija, većina koristi pristup koji se zasniva na riziku kako bi procijenila valjanost svojih nalaza. Konkretno, ocjenjuju rizik da finansijski izvještaji koji im se dostavljaju nisu tačni. To revizori rade tako što procjenjuju, između ostalog, računovodstvene procedure i procedure izvještavanja agencije, slabosti njene unutarnje kontrole, ali i slabosti vlastitih procedura za otkrivanja nepravilnosti i nezakonitosti.

Revizija rada obavještajnih službi može biti veoma izazovan zadatak iz razloga koji se razmatraju u 2. dijelu ovog poglavlja, pogotovo neizvjesnosti ishoda i neopipljivosti koristi koje karakteriziraju obavještajni rad. Glavne revizorske institucije mogu naići na poteškoće, npr. prilikom procjene vrijednosti operativnih aktivnosti (kao što je vođenje i nadzor agenata) čiji se uspjeh ili neuspjeh teško može kvantitativno odrediti. Kao rezultat toga, neke glavne institucije se uzdržavaju od procjene rada u tim područjima.

Revizije koje su usmjerene na učinak mogu, međutim, proizvesti nalaze koje ne mogu proizvesti drugi tipovi revizije. Razmotrite, na primjer, slučaj velikog kapitalnog projekta ili velikog programa nabavki koji prolazi finansijsku i zakonsku ocjenu zato što je propisno obračunat te je ispoštovao sve važeće zakone i propise. Ovi projekti i programi, ipak, mogu biti malog učinka, odnosno slabe vrijednosti za potrošeni novac – što je neuspjeh koji bi se otkrio samo ako bi se obavila revizija učinkovitosti.

U mjeri u kojoj glavne revizorske institucije provode reviziju učinka obavještajnih službi, one obično usmjeravaju pažnju na specifična pitanja ili teme u više agencija (vidjeti Okvir 7) – kao što su sistemi informacijske tehnologije ili procedure sigurnosne provjere.

Okvir 7: Revizija učinka u Kanadi

Glavni revizor Kanade je 2004. godine proveo reviziju učinka kanadske Obavještajne i sigurnosne službe i drugih agencija koje su vezane za obavještajni rad. Ova revizija razmotrila je „ukupno upravljanje Inicijativom javne sigurnosti i antiterorizma [i] koordinaciju obavještajnog rada među odjelima i agencijam,a te njihovu sposobnost da daju adekvatne informacije uposlenim u organima za provedbu zakona."[39] To se desilo nakon značajnih investicija uloženih u borbu protiv terorizma koje je Vlada Kanade donijela nakon 11. septembra.

U završnom revizorskom izvještaju, glavni revizor je zaključio, između ostalog, da „vlada nije imala okvir upravljanja kojim bi se rukovodila prilikom donošenja odluka o investicijama, upravljanju i razvoju, koji bi joj omogućio da provodi i usmjerava komplementarne akcije u zasebnim agencijama."[40] Nadalje, prema glavnom revizoru, „vlada u cjelini nije uspjela postići poboljšanje u sposobnosti sigurnosnog informacijskog sistema da komunicira međusobno."[41] Generalno govoreći, glavni revizor je ustanovio da je bilo „nedostataka u načinu kako se obavještajnim radom upravljalo u cijeloj Vladi."[42]

6.5 PRISTUP INFORMACIJAMA

Glavnim institucijama za reviziju potreban je neograničen pristup informacijama, što je preduslov za visokokvalitetnu reviziju, ali i garancija operativne nezavisnosti. Razumljiva želja obavještajne službe da zaštiti povjerljive informacije od neovlaštenog otkrivanja ne umanjuje tu potrebu glavnih institucija za reviziju. Prema tome, dobra praksa zahtijeva da važeći zakon pruži glavnim institucijama za reviziju pristup svim dokumentima, osobama

i fizičkim lokacijama koje revizori smatraju potrebnim u svom radu. Ovo je, na primjer, slučaj Južne Afrike (vidjeti Okvir 8), kao i Njemačke (vidjeti Okvir 9), gdje takav pristup uključuje informacije o tekućim obavještajnim operacijama. Bitno je, ali ne i dovoljno da se taj pristup ugradi u zakon(e) koji reguliraju rad glavnih revizorskih institucija. Zakonodavci moraju također osigurati da zakoni o obavještajnim službama i klasificiranim informacijama ne budu u suprotnosti sa odredbama koje definiraju pravo pristupa za glavne revizorske institucije. Zakon treba ovim institucijama dati i ovlasti koje su osmišljene radi podrške njihovom pristupu informacijama. Te ovlasti mogu uključiti ovlast da se naloži obavezno svedočenje i davanje dokaznog materijala, te ovlast da se vrše pretres i zapljena (vidjeti Okvir 8).

Okvir 8: Ovlasti glavnog revizora Južne Afrike[43]

Teoretski, glavni revizor Južne Afrike ima velike ovlasti koje on ili ona može koristiti da bi dobio pristup potrebnim informacijama. Ovaj okvir sumira te ovlasti. Treba zapaziti, međutim, da u praksi uključivanje takvih ovlasti u pravni okvir za glavnog revizora ne garantira neophodno otkrivanje relevantnih informacija od strane obavještajnih službi čiji je rad obavijen velom tajne.[44]

Pristup informacijama

Važeći zakon pruža glavnom revizoru prilikom obavljanja revizije puni i neograničeni pristup u svako razumno vrijeme:

- bilo kojem dokumentu, pisanom ili elektronskom zapisu, ili drugim informacijama koje su u posjedu agencije koja je pod revizijom, koja otkriva poslovanje, finansijsku aktivnost, finansijsku poziciju ili rad te institucije;
- bilo kojem sredstvu institucije koja je predmet revizije ili sredstvima koja su pod njenom kontrolom;
- bilo kojem predstavniku te institucije ili njenom uposleniku.

Ovlasti revizije

Kada obavlja reviziju, glavni revizor može:

- naložiti osobi da otkrije pod zakletvom, bilo usmeno ili pismeno, informacije koje mogu biti relevantne za reviziju – uključujući povjerljive, tajne ili klasificirane informacije;
- ispitati bilo koju osobu o tim informacijama.

Usto, kada obavlja reviziju, glavni revizor može dobiti od sudije nalog da:

- uđe u bilo koji posjed, prostorije ili vozilo na osnovu opravdane sumnje da se relevantne informacije čuvaju ili su sakrivene u njima;
- pretraži bilo koji posjed, prostorije ili vozilo, kao i bilo koju osobu u prostorijama ili vozilu radi potencijalno relevantnih informacija;
- zaplijeni bilo koje potencijalno relevantne informacije u svrhu obavljanja revizije.

Općenito, glavni revizor ima pravo pristupa potrebnim informacijama koje je starije od obaveze obavještajne službe da sačuva povjerljivost. Na primjer, od osobe koju važeći zakon obavezuje da ne otkrije informaciju vezanu za neko obavještajno pitanje, može se ipak zatražiti da otkrije tu informaciju glavnom revizoru. U takvim slučajevima, ispunjavanje zahtjeva glavnog revizora se ne smatra kršenjem obaveze da ne otkrije informaciju koju ta osoba ima.

U nekim državama, zakon nameće ograničenja na pristup informacijama glavnih revizorskih institucija. To se odnosi na Državni ured za reviziju Ujedinjenog Kraljevstva, na primjer, koji ima ograničen pristup informacijama koje se odnose na obavještajne izvore i metode. Ovo ograničenje je usko i jasno definirano, i nije osmišljeno kako bi onemogućilo rad Državnog ureda za reviziju. Drugdje, međutim, ograničenja pristupa informacijama glavnim institucijama za reviziju su mnogo šira. U SAD, na primjer, zakon omogućava obavještajnoj zajednici značajno diskreciono pravo u odlučivanju koje informacije će razmijeniti sa Vladinim uredom za odgovornost (GAO), i to na osnovu pojedinačnih slučajeva.[45] Nadalje, GAO nema dozvolu da pristupi informacijama koje se odnose na "lažne račune", metode, i tajne akcije.[46] Ograničenja na pristup informacijama onemogućavaju rad GAO-a i njegovih partnera u drugim zemljama. Ona mogu smanjiti učinkovitost i sveobuhvatnost nezavisnog finansijskog nadzora.

Čak i kada važeći zakon glavnim revizorskim institucijama daje velike izvršne ovlasti, te ovlasti možda neće biti dovoljne da osiguraju pristup svim informacijama koje glavna revizorska institucija smatra relevantnim. Zbog povjerljive prirode mnogih pitanja vezanih za obavještajne službe, glavne revizorske institucije suočene su sa značajnim praktičnim preprekama u pristupu određenim tipovima informacija. Treba reći da one imaju poteškoća kada treba da obave razgovore sa plaćenim doušnicima, ili da dobiju informacije o tajnim operacijama, te kada verificiraju postojanje sredstava koja koriste povjerljivi agenti.

Utjecaj na revizije ovih pravnih i praktičnih ograničenja zavisi, između ostalog, od tipa revizije koja se provodi i spremnosti obavještajne službe na saradnju. U nekim okolnostima, ograničenja u pristupu informacijama mogu znatno onemogućiti sposobnost glavne revizorske institucije da obavlja svoj rad, te podrivati integritet procesa revizije i rezultirati u nižem od željenog nivoa sigurnosti revizije. To je posebno problematično ako revizori nisu svjesni da su informacije, koje bi mogle dovesti do izmjene njihovih zaključaka, bile od njih sakrivene. U odsustvu takvih informacija, oni mogu čak dati nekvalificirano mišljenje koje daje lažni osjećaj odgovornosti.

Problemi ove vrste najvjerovatnije će se pojaviti u zemljama gdje autoritet i nezavisnost glavne revizorske institucije nije u potpunosti uspostavljena i/ili tamo gdje glavna revizorska institucija ima neprijateljski odnos sa obavještajnim službama koje su predmet njihove revizije. Ukoliko glavna revizorska institucija utvrdi da su ograničenja njenom pristupu informacijama umanjila njenu sposobnost da izda precizno revizorsko mišljenje, međunarodni revizorski standardi zahtijevaju od te glavne revizorske institucije da izda tzv. kvalificirano mišljenje (eng. qualified opinion), koje sadrži napomenu da je ono sačinjeno sa ograničenim pristupom informacijama. Poštivanje te profesionalne dužnosti osigurava da bilo koja pravna ili praktična ograničenja na pristup informacijama budu uključena kao faktor u revizorskim mišljenjima i izvještajima.

6.6 ZAŠTITA INFORMACIJA

Kako bi se osiguralo i obavještajnim službama i izvršnoj vlasti da informacije otkrivene revizorima ostanu povjerljive, mnoge glavne revizorske institucije uspostavile su specijalne odjele sa sigurnim prostorijama i uposlenicima koji su sigurnosno provjereni kako bi mogli da obavljaju obavještajne revizije. (Kao opće pravilo, uposlenici glavnih institucija za reviziju koji vrše revizije evidencija obavještajnih službi moraju se pridržavati istih sigurnosnih standarda kao i uposlenici samih službi koji imaju pristup istim evidencijama – uključujući zakonsku obavezu da štite tajnovitost klasificiranih i drugih povjerljivih

informacija[47]). Korištenje povjerljivih informacija na profesionalan način gradi povjerenje između glavnih institucija za reviziju i obavještajnih službi, te povećava vjerovatnoću da će informacije spremno biti date i u budućnosti.

6.7 IZVJEŠTAJI

Izvještaji su prvenstveno sredstvo kojim revizori iznose svoje nalaze i preporuke. Oni koji čitaju revizorske izvještaje uključuju rukovodstvo obavještajne službe, zvaničnike izvršne vlasti, parlamentarce i pripadnike javnosti. Često, ti akteri preduzimaju akciju prvenstveno na osnovu izvještaja glavnih institucija za reviziju koje pročitaju. Još značajnije, parlamentarci koriste ove izvještaje kao osnov za vlastiti nadzor nad finansijama obavještajnih službi. I doista, prvenstveno kroz parlamentarne odluke o budućim budžetima, nalazi glavnih institucija za reviziju i njihove preporuke mogu imati utjecaja na obavještajne službe i izvršnu vlast.

6.7.1 Tajnost

Pošto izvještaji glavnih institucija za reviziju o obavještajnim službama sadrže reference na klasificirane informacije, neprečišćena verzija obično se ne podnosi javnosti, a čak ni većini članova parlamenta. Važeći zakon obično ograničava ko prima potpune (klasificirane) izvještaje od višeg rukovodstva službe, viših vladinih zvaničnika, članova parlamentarnog odbora za nadzor, te, u nekim slučajevima, članova parlamentarnih odbora za finansije/budžet.

Mada osjetljive informacije o državnoj sigurnosti koje su sadržane u izvještajima glavne revizorske institucije treba svakako da ostanu u „krugu tajnosti“, ima mnogo segmenata tih izvještaja koji mogu i treba da budu izneseni u javnost. U tom pogledu, glavni revizor Južne Afrike je naveo da njegovi izvještaji o obavještajnim službama treba da budu javni zato što u njima nema ništa što bi, ako bi bili otkriveni, izazvalo loše stavove o službama ili ugrozilo sigurnost zemlje.[48]

Blanko zabrane na objavljivanje revizija obavještajnih službi te rutinska klasifikacija njihovog sadržaja odriču temeljne demokratske principe transparentnosti, otvorenog vladanja, i slobode informacija. U pogledu ovog pitanja, Ustav Južne Afrike je posebno napredan jer zahtijeva otkrivanje svih izvještaja koje pripremi revizor, uključujući i one koji se odnose na obavještajne službe, pri čemu se osjetljive informacije mogu ukloniti.[49] Općenito, tajnost treba da bude izuzetak od općeg pravila o objavljivanju i treba biti dozvoljena samo kada je potrebna radi zaštite legitimnih interesa državne sigurnosti.

Ni u kojem slučaju članovi obavještajnih službi, niti izvršna vlast ne smiju biti u prilici da koriste odredbe o tajnosti kako bi sakrili nezakonito korištenje javnih sredstava. Dobra praksa zahtijeva da važeći zakon sadrži jasnu odredbu koja omogućava otkrivanje klasificiranih informacija, kada je to potrebno, kako bi se otkrila takva neprihvatljiva djela. Ovakva formulacija u Zakonu o javnoj reviziji Južne Afrike opisuje kada se to traži:

> *(1) Glavni revizor mora preduzeti mjere predostrožnosti kako bi spriječilo otkrivanje tajnih ili klasificiranih informacija ….*
>
> *(2) Koraci preduzeti u pogledu stava (1) ne mogu spriječiti otkrivanje bilo kojeg revizorskog nalaza od strane glavnog revizora ili ovlaštenog revizora oko bilo kakve neovlaštene potrošnje, nepropisne potrošnje ili neopravdane potrošnje... ili bilo*

kakvog drugog nepropisnog ili kriminalne aktivnosti vezane za finansijske poslove agencije koja je predmet revizije, ali svako takvo otkrivanje ne može uključiti činjenice čije otkrivanje bi ugrozilo nacionalni interes.[50]

6.7.2 Objavljivanje informacija

Glavne revizorske institucije trebalo bi, minimalno, podnijeti javnosti sljedeće tipove informacija o svojim revizijama/pregledima agencijskih službi:

- *spisak revizija koje je obavila ili će obaviti glavna revizorska institucija* - referenca može biti jednostavna, na primjer, naslov i kratko objašnjenje;[51]
- *osnovno mišljenje revizije o finansijskim izvještajima službe* - najčešće vrlo kratak dokument kojim se otkriva malo informacija, ali se potvrđuje da je došlo do interakcije sa datom službom;
- *javne verzije klasificiranih izvještaja* - glavne revizorske institucije treba da objavljuju javne verzije svojih izvještaja, uključujući periodične revizije i revizije učinka koje se odnose na obavještajne službe (vidjeti Okvir 7, na primjer). To se može uraditi kroz redakciju (uklanjanje) osjetljivih informacija iz klasificiranih verzija izvještaja, izrada posebnih javnih verzija izvještaja, ili uključivanjem svih klasificiranih informacija u anekse koji neće biti objavljeni. Dok većina parlamenata i stručnih nadzornih tijela objavljuju javne verzije svojih izvještaja, ova praksa još uvijek nije postala raširena među glavnim institucijama za reviziju.

6.8 VAŽNOST TRANSPARENTNOSTI U RADU GLAVNIH INSTITUCIJA ZA REVIZIJU

Kako bi se pridržavalo principa demokratskog upravljanja, javnost treba znati koliko je moguće više – što je podložno ograničenjima u pogledu povjerljivosti koja smo ranije razmatrali – o radu glavnih institucija za reviziju i njihovim izvještajima o obavještajnim službama. Izvještavanje javnosti o reviziji provedenoj u obavještajnoj službi, koje provode glavne revizorske institucije, pomaže jačanju povjerenja u, i podrške - kako službama koje su predmet revizije, tako i glavnih institucija za reviziju. Uvjeravanje javnosti da je obavještajna zajednica predmet propisne kontrole, doprinosi korisnoj percepciji da obavještajne službe djeluju profesionalno, koriste javna sredstva na propisan način te da djeluju u okvirima zakona.

Štaviše, transparentnost pomaže da se razbiju mitovi o obavještajnim službama – koji se posebno tiču njihovog korištenja javnih sredstava. Ovo je osobito potrebno u zemljama u kojima je nivo povjerenja u obavještajne službe i dalje nizak i gdje su one ranije vršile zloupotrebu sredstava. Ona također koristi da bi se potaknula javna debata i da bi ona bila zasnovana na dobroj obaviještenosti o propisnoj ulozi obavještajnih službi. To može biti važno kada su vlade suočene sa velikim budžetskim deficitima i moraju rezati budžete javnih službi.

Okvir 9: Njemački Savezni sud za reviziju

Na temelju Ustava Njemačke uspostavljen je Savezni sud za reviziju (FCA), kao nezavisno tijelo sa zadatkom revizije svih vladinih agencija, uključujući tri savezne obavještajne službe.[52]

Funkcije

Dužnosti FCA u pogledu javnih agencija uključuju:

- reviziju njihovog prihoda, rashoda, aktive i pasive, te razmatranje bilo kojih akcija koje su one preduzele a koje mogu imati finansijske posljedice;
- podrška Parlamentu u provođenju njegovog prava da utvrđuje budžete agencija,
- podrška Parlamentu prilikom odlučivanja da li dati sredstva izvršnoj vlasti u pogledu njenog upravljanja javnim sredstvima.[53]

Opseg revizije

Važeći zakon ne nameće ograničenja u pogledu aktivnosti FCA. Prema tome, FCA sama odlučuje o tome koje agencije će biti predmet njene revizije i kada i kako će se revizija izvršiti. Članovi parlamenta mogu zahtijevati revizije FCA, ali ne mogu primorati FCA da nešto uradi.

Revizije koje obavlja FCA utvrđuju da li su agencije poštovale zakone i propise u vezi sa finansijskom aktivnošću. Posebno, one utvrđuju:

- da li su odredbe zakona o budžetu bile poštovane;
- da li su evidencije o agencijskom prihodu, rashodu, aktivi i pasivi uredne i propisno potkrijepljene dokumentima;
- da li se javnim sredstvima upravljalo djelotvorno;
- da li su dodijeljeni zadaci učinkovito obavljeni.

Obavještajna pitanja koja pokrene FCA često se upućuju na Povjerljivi odbor Bundestaga (vidjeti Okvir 5), i o njima se kasnije raspravlja u okviru rasprave o budžetu. Prema tome, predstavnici glavne revizorske institucije često učestvuju na sastancima Povjerljivog odbora, čime se stvara i korisna veza između revizije i procesa odlučivanja o budžetu.[54]

Sastav

FCA predvodi predsjednik i potpredsjednik. Obojicu imenuje izvršna vlast, a bira parlament. Svaki od njih ima mandat od maksimalno dvanaest godina. FCA je podijeljen po tematskim odjelima, od kojih svaki ima direktora i njegovog ili njenog zamjenika. Svi ovi ljudi su "članovi suda", što znači da uživaju sudsku nezavisnost. Većina odluka koje se tiču revizije donosi se u "kolegijima" od dva člana suda (relevantni direktor i šef odjela), a tamo gdje ima neslaganja, pridružuje im se predsjednik te se tako formira kolegij trojice.[55]

Pristup informacijama

Važeći zakon obavezuje sve vladine agencije, uključujući obavještajne službe, da FCA dostave bilo koji dokument koji on smatra potrebnim kako bi obavio svoj rad. Nema ograničenja na ovu obavezu.[56]

Izvještaji

Dok FCA obično daje svoje nalaze na uvid javnosti, njegovi izvještaji o obavještajnim službama se ne podnose javnosti. Umjesto toga, oni se podnose povjerljivom odboru, Odboru za nadzor nad obavještajnim službama Bundestaga te relevantnim izvršnim tijelima.[57]

7. PREPORUKE

Mada nema jednog jedinog „najboljeg“ pristupa nadzoru nad finansijama obavještajnih službi, sljedeće preporuke, izvučene iz zakona, institucionalnih modela i praksi o kojima se razmatralo u ovom dokumentu, predstavljaju dobre prakse koje se mogu prilagoditi kako bi se uklopili u mnoge različite pravne i institucionalne modele. Većina ovih preporuka pretpostavlja da pravni i institucionalni okvir za budžet i reviziju već postoje, te da je važeći zakon u pogledu upravljanja i korištenja javnim sredstvima već uveden.

Preporuke vezane za budžet i finansijske izvještaje

- Budžeti obavještajnih službi treba da budu „sveobuhvatni“ što znači da treba da obuhvate sve finansijske aktivnosti službe. Važeći zakon treba posebno zabraniti da se službe angažiraju u finansijskoj aktivnosti koja nije uključena u njihov budžet.
- Vlade treba da otkriju koliko je moguće više informacija o budžetu obavještajne službe, a da pri tome ne ugroze javnu ili državnu sigurnost. Kao minimum one treba da otkriju ukupni iznos koji je raspodjeljen službi, iznose po pojedinim kategorijama troškova, te ciljeve vezane za određene rashode. Informacije o budžetu treba da budu klasificirane samo tamo gdje je tajnost striktno potrebna kako bi se zaštitili legitimni interesi državne sigurnosti.
- Parlamenti treba da usvoje zakon koji određuje koje finansijske informacije (uključujući budžete i finansijske izvještaje) moraju biti otkrivene, a koje moraju ostati povjerljive i/ili predmet izuzetnih procedura računovodstva i revizije.
- Obavještajne službe treba da pripreme javne verzije svojih finansijskih izvještaja koje sadrže što je moguće više informacija.

Preporuke vezane za unutarnje finansijske kontrole

- Obavještajne službe ne smiju biti izuzete od zakona koji reguliraju unutarnje finansijske kontrole i mehanizme revizije javnih agencija.
- Ako se obavještajnoj službi dozvoli povremeno odstupanje od zakona i propisa o upravljanju i korištenju javnih sredstava, ovlaštenje da se takvo odstupanje dopusti treba da bude zakonski utemeljeno.

Preporuke vezane za vanjski finansijski nadzor

- Relevantni zakon treba da zahtijeva od glavnih institucija za reviziju da provode reviziju finansija obavještajnih službi kako bi utvrdile da li su finansijski izvještaji službe tačni i ispravni, da li su finansijske transakcije službe usklađene sa važećim zakonima i propisima, te da li se javna sredstva koriste učinkovito na način koji pruža najveću vrijednost za uloženi novac. U postizanju tih ciljeva, glavne revizorske institucije treba da imaju ovlast da provode reviziju svih aspekata aktivnosti službe, uključujući specijalne račune vezane za tajne ili inače osjetljive operacije.
- Parlamenti i glavne revizorske institucije treba da podvrgnu finansije obavještajnih službi istom nivou kontrole koja se primjenjuje na finansije drugih javnih agencija. Ova kontrola treba da se odvija tokom cijelog budžetskog ciklusa, počevši sa punom

ocjenom klasificiranih dijelova budžetskog prijedloga, te zaključno sa naknadnom ocjenom i revizijom finansijskih izvještaja službi.

- Važeći zakon treba da pruži vanjskim nadzornim tijelima pristup svakoj informaciji koju smatraju potrebnom da bi obavili svoj rad, bilo da je ta informacija u posjedu obavještajne službe koja je predmet revizije ili bilo kojeg drugog javnog tijela. Takav pristup treba da bude podržan odgovarajućim istražnim ovlastima dovoljnim da se zahtijeva davanje informacija.
- Parlamenti i glavne revizorske institucije sa pristupom povjerljivim informacijama treba da preduzmu korake da zaštite te informacije od neovlaštenog otkrivanja. Takve mjere treba da osiguraju da se informacije stave na raspolaganje samo uposlenicima koji ih trebaju znati, da su fizički i tehnički bezbijedne, i da postoje sankcije kako bi se odvratilo od neovlaštenog otkrivanja.
- Članovi parlamentarnih odbora odgovorni za finansijski nadzor treba da imaju dovoljno ljudskih i tehničkih kapaciteta koji će im omogućiti da razumiju finansije obavještajne službe i provode kontrolu na svrsishodan način.
- Parlamenti treba da osiguraju da glavne revizorske institucije imaju ovlasti i sredstva potrebna da obave svoj rad. Nadalje, oni treba da promoviraju provedbu preporuka glavnih institucija za reviziju od strane obavještajnih službi.
- Parlamenti treba da osiguraju da postoje odgovarajuće veze između vanjskih tijela za nadzor tako da se rezultati naknadnih ocjena i revizija mogu koristiti kako bi se na pravi način vršila kontrola budžetskih prijedloga u sljedećim godinama.
- Parlamentarni odbori odgovorni za finansijski nadzor nad obavještajnim službama treba da se aktivno angažuju sa glavnim institucijama za reviziju, što treba da uključi: pregled njihovih izvještaja, održavanje kasnijih sastanaka i preduzimanje koraka da se osigura da glavne revizorske institucije imaju adekvatne ovlasti i sredstva kako bi valjano obavile reviziju obavještajnih službi.
- Parlamenti i glavne revizorske institucije imaju odgovornost da obavještavaju javnost o svom nadzoru nad obavještajnim službama. Oni treba da pripreme javne verzije svojih nalaza te podnose periodične izvještaje javnosti o svojim aktivnostima.

Bilješke

1. Ovo poglavlje rezultat je toka i pisanih priloga za DCAF-ovu radionicu o finansijskom nadzoru nad obavještajnim službama. Među učesnicima su bili viši predstavnici vrhovnih revizorskih institucija, po jedan predstavnik državnog parlamenta, bivši obavještajni zvaničnici i predstavnici akademske zajednice iz cijelog niza zemalja. Sva izlaganja su bila off the record i stoga nisu direktno citirana. Učesnici su također dali korisne povratne informacije za nacrt ovog poglavlja. Autor bi želio izraziti zahvalnost svim članovima ove grupe, a također zahvaljuje svojim kolegama u DCAF-u Hans Born, Benjamin S. Buckland i Gabriel Geisler na njihovim dragocjenim komentarima na prve nacrte. "Vrijednost za novac" odnosi se na ekonomičnost, efikasnost i učinkovitost sa kojom jedna organizacija koristi vlastita sredstva u obavljanju svojih odgovornosti: vidjeti "Performance Audit" u: International Organization of Supreme Audit Institutions, Financial Audit Guideline – Glossary of Terms to the INTOSAI Financial Audit Guidelines.
2. Sjedinjenje Države, Central Intelligence Agency; appropriations; expenditures, U.S. Code 50 §403j (dostupno na http://us-code vlex.com/vid/central-intelligence-agency-expenditures-19266900).
3. Za primjere tih izuzetaka, vidjeti United Kingdom, The Defence and Security Public Contracts Regulations 2011, No. 1848, Čl. 7 (dostupno http://www.legislation.gov.uk/uksi/2011/1848/made).
4. Glavni revizor Kanade, "Chapter 27—The Canadian Intelligence Community—Control and Accountability," u *Report of the Auditor General of Canada* (1996) Čl. 27.107 (dostupno na http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_27_e_5058.html).
5. Za detaljnije informacije, vidjeti David Johnston i Mark Mazzetti, "A Window Into C.I.A.'s Embrace of Secret Jails," *New York Times, 12*. avgust 2009; vidjeti i David Johnston, "Ex-C.I.A. Official Admits Corruption," *New York Times, 29*. septembar 2008; Matthew Barakat, "Feds: Misconduct by CIA's Foggo spanned decades," *Associated Press*, 25. februar 2009; i *U.S. v. Foggo and Wilkes*, U.S. District Court of Southern California, Grand Jury Indictment, juni 2005.
6. The World Bank, "Code of Practices on Fiscal Transparency," in *Public Expenditure ManagementHandbook* (Washington, DC: The World Bank, 1998), Annex J.
7. Todor Tagarev, (ed.), *Building Transparency and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), str. 64. Za primjer iz državnog zakona, vidjeti South African Public Finance Management Act,br. 1 iz 1999, Čl. 38(2).
8. Todor Tagarev, (ed.), *Building Transparency and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), str. 64. Za primjer iz državnog zakona, vidjeti Zakon o upravljanju javnim finansijama Južne Afrike,br. 1 iz 1999, Čl. 38(2).
9. Za detaljniju diskusiju o raznim pristupima budžetskom procesu, vidjeti The World Bank, *Public Expenditure ManagementHandbook*, str. 12–16; Tagarev, *Building Transparency*,str. 59; i Organisation for Economic Co-operation and Development (OECD), "Performance Budgeting: A User's Guide," Policy Brief (mart 2008).
10. Jedinstveni račun za obavještajne službe UK daje zbirni budžet za tri civilne obavještajne službe.
11. Za detaljniju diskusiju, vidjeti Nicolas Masson i Lena Andersson, *Guidebook: Strengthening Financial Oversight in the Security Sector* (Geneva: DCAF, 2012).
12. Francuska, Mission Ministérielle Projets Annuels de Performances, "Annexe au projet de loi de finance pour Défense"(2010), str. 36¬–37.
13. O značaju potreba da oni koji donose odluke imaju pristup svim informacijama o budžetu, vidjeti:The World Bank, *Public Expenditure ManagementHandbook*, str. 1–2.
14. Ured SAD za računovodstvo (United States General Accounting Office), "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (juli 2001), str.10; i United States, Central Intelligence Agency; appropriations; expenditures, Zakon S.A.D. 50 §403j.
15. Vidjeti npr. Australija, Financial Management and Accountability Act 1997, Čl. 49.
16. Sigurnosno-obavještajna agencija Australije, Finansijski izvještaji u *Annual Report 2010-11* (Canberra: 2011), str. 133–151 (dostupno na http://www.asio.gov.au/img/files/Report-to-Parliament-2010-11.pdf).
17. Francuska, Loi organique n°2001¬–692 du 1 août 2001 relative aux lois de finances (LOLF), Čl. 54.
18. Za diskusiju o italijanskom modelu po kojem Parlament glasa o zbirnom iznosu, a specifične raspodjele sredstava ostaju diskreciono pravo izvršne vlasti, vidjeti Federico Fabbrini i Tomasso Giupponi, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Italy," u knjizi Aidana Willsa i Mathiasa Vermeulena, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (Brussels: European Parliament, 2011), Annex A, str.245.
19. Mađarska, Zakon CXXV iz 1995 o Državnim

sigurnosnim službama, Čl. 14(g).

20. Richard Best, *The Intelligence Appropriations Process: Issues for Congress* (Washington, DC: Congressional Research Service, 27. oktobar 2011); vidjeti i Richard Best and Elizabeth Bazan, *Intelligence Spending: Public Disclosure Issues* (Washington, DC: Congressional Research Service, February 15, 2007), str. 5; Frederick Kaiser, Walter Oleszeck i Todd Tatelman, *Congressional Oversight Manual, Congressional Research Service* (Washington, DC: Congressional Research Service, June 2011), str. 16–19; Eric Rosenbach i Aki Peritz, *Confrontation or Collaboration? Congress and the Intelligence Community* (Cambridge, MA: Harvard, 2009), str. 24–28; i James Saturno, *The Congressional Budget Process: A Brief Overview* (Washington, DC: Congressional Research Service, 2004).
21. Njemački Savezni zakon o budžetu, Čl. 10(a). Vidjeti i Hans De With i Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany," u knjizi Willsa I Vermeulena, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Annex A, str. 225–226.
22. Za detaljniju diskusiju, vidjeti Wills i Vermeulen, str. 129–131.
23. Italija, Zakon 124/2007, Čl. 33(8) i 29(2).
24. Španija, Ley 11/1995, Čl., 2.2. Vidjeti i Susana Sanchez Ferro, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Spain," u knjizi Willsa I Vermeulena, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aneks A, str. 271.
25. Predsjedavajući Odbora za javne račune uvijek je iz opozicije.
26. Ujedinjeno Kraljevstvo, Zakon o obavještajnim službama iz 1994, Čl. 10 (1).
27. Vidjeti, npr. Ujedinjeno kraljevstvo, Odbor za obavještajne službe i sigurnost, *Annual Report 2010–2011*, CM 8114 (2011), str. 12–16.
28. Ian Leigh, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in the United Kingdom," u knjizi Willsa I Vermeulena, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, str. 298.
29. Ibid, str. 297. Primjeri rada istražitelja su razmatrani u knjizi Ujedinjeno kraljevstvo, Odbor za obavještajne službe i sigurnost, Annual Report 2010–2011, CM 8114 (2011), str. 7, 16, 17 i 79.
30. OECD, "Relations Between Supreme Audit Institutions and Parliamentary Committees," Sigma Papers, br. 33 (Paris: OECD Publishing, januar 2002), str. 19–20.
31. U nekim zemljama, parlamentarna ex post provjera utvrđuje da li je glavna revizorska institucija uradila svoj posao na propisan način.
32. Francuska, Ministarstvo za budžet, javne račune i državnu službu, "Guide to the Constitutional Bylaw on Budget Acts" (2008) str. 32; Francuska, LOLF, Čl. 54. i Čl. 58; United States, Government Accountability Office web site (dostupno na http://www.gao.gov/about/index.html).
33. Njemačko Savezno ministarstvo finansija, "The Budget System of the Federal Republic of Germany" (Berlin: 2008) str. 47.
34. UN General Assembly Resolution, "Promoting the efficiency, accountability, effectiveness and transparency of public administration by strengthening supreme audit institutions," United Nations Document A/RES/66/209 (15. mart 2012),.
35. Ibid., str. 18.
36. Ovo se i dalje odnosi na SAD, gdje je ovlast glavnog revizora da vrši reviziju nekoliko oblasti rada CIA-e ograničen i u praksi i po zakonu. Vidjeti Intelligence Community Directive, br. 114, 30. juni 2011; Gene Dorado (US Comptroller General), Letter to Director of National Intelligence James Clapper regarding "GAO Comments on Intelligence Community Directive Number 114: Comptroller General Access to Intelligence Community Information," 28. april 2011; i US GAO, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (juli,2001), str. 4–8.
37. France, Loi n° 2001–1275 du 28 décembre 2001 de finances pour 2002, Article 154; France, L'Assemblée Nationale, "Rapport fait au nom de la Commission des Finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2012: Annexe n° 12, direction de l'action du gouvernement publications officielles et information administrative" (14. oktobar 2009), str. 25–27.
38. Sjedinjene Države, Auditing Expenditures Approved Without Vouchers, U.S. Code 31 §3524.
39. Ured glavnog revizora Kanade, *mart 2004 Report of the Auditor General of Canada* (2004), Čl. 3.2.
40. Ibid, Čl. 3.3.
41. Ibid, Čl. 3.4.
42. Ibid, Čl. 3.5.
43. Južna Afrika, Zakon o javnoj reviziji, br. 25 iz 2004, Čl. 15–16.
44. Južna Afrika, Ministarska komisija za provjeru obavještajnih službi, *Intelligence in a Constitutional Democracy* (Pretoria: septembar 2008), str.

226–227.

45. Intelligence Community Directive, br. 114; and Gene Dorado, Letter to Director of National Intelligence James Clapper, 28. april 2011.
46. Gao Sjedinjenih Država, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," str. 4–8; Intelligence Community Directive, br. 114; i Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles against an Overpowering Force," *International Journal of Intelligence and Counterintelligence* Vol. 15, br. 3 (Fall 2002): str. 345–353.
47. Vidjeti, npr, Australijski zakon o Uredu glavnog revizora 1997, Čl. 36; 31 U.S.C. 716; i OECD "The audit of secret and politically sensitive subjects, comparative audit practices," Sigma Papers, br. 6 (Paris: OECD Publishing, 1996), str. 12.
48. Južna Afrika, Ministarska komisija za provjeru obavještajnih službi, *Intelligence in a Constitutional Democracy* (Pretoria: septembar 2008), str. 229.
49. Ustav Republike Južne Afrike, br.108, 1996, Čl. 188(3).
50. Južna Afrika, Zakon o javnoj reviziji, Čl. 18.
51. Australijski Državni ured za reviziju primjenjuje ovu praksu. Primjer jednog njegovog plana revizije može se naći na http://www.anao.gov.au/~/media/Files/Audit%20Work%20Programs/2011_Audit_Work_Plan.PDF. Primjer kako jedan državni ured za reviziju radi reviziju tokom operacije može se naći na http://www.anao.gov.au/Publications/Audits-in-Progress.
52. German Basic Law, Čl. 114(2); Njemačka, Savezni zakon o budžetu od 19. avgusta 1969, *Savezni službeni list I*, str. 1284, kako je nedavno dopunjen Čl. 4 Zakona od 31. jula 2009, *Federal Law Gazette I*, str. 2580, Čl. 10a (3); Čl. 88.
53. German Basic Law, Čl. 114(2); Audit Rules of the Bundesrechnungshof (Germany's Federal Court of Audit), posljednji put dopunjen odlukom Senata od 29/30. avgusta 2005, Čl. 3, 56–57.
54. Njemačka, Federal Budget Code, Čl. 10a (3) i 89–90; Audit Rules of the Bundesrechnungshof, Articles 4–5; The Budget System of the Federal Republic of Germany, str. 49 i 51.
55. German Federal Court of Audit Act od 11. jula 1985. (BGBl. I 1985, str. 1445) kako je posljednji put dopunjen Čl.om 17. Zakona od 9. jula 2001 (BGBI. I, str. 1510), Čl. 3, 5, 6, 9 i 19.
56. Njemačka, Federal Budget Code, Čl.10a (3) i 95
57. Njemačka, Federal Budget Code, Čl. 10a (3); Audit Rules of the Bundesrechnungshof Čl. 50.

POGLAVLJE 9

Rješavanje žalbi na obavještajne službe

Craig Forcese

DEVET

9

Rješavanje žalbi na obavještajne službe

Craig Forcese

1. UVOD

Ovaj tekst se bavi ulogom nadzornih tijela u rješavanju žalbi na obavještajne službe koje podnose pripadnici javnosti, kao i žalbi koje podnose pripadnici obavještajnih službi. Potreba za sistemom rješavanja žalbi je posebno važna kad su u pitanju obavještajne službe zato što one „često imaju izuzetne ovlasti, kao što su tajno prikupljanje podataka ili sigurnosna provjera, koje, ako se koriste nepropisno ili pogrešno, nose sa sobom rizik nanošenja ozbiljne nepravde za pojedince.[1] Međutim, potreba za sistemom rješavanjem žalbi ide dalje od od nuđenja pravnih lijekova za prekršena prava. Mehanizmi rješavanja žalbi za obavještajne službe „mogu također pojačati odgovornost time što će naglasiti administrativne greške i lekcije koje treba naučiti, što vodi do poboljšanog rada."[2]

Iz ovih i drugih razloga, sistemi rješavanja žalbi se smatraju suštinskim dijelom upravljanja obavještajnim službama. U tom pogledu, specijalni izvjestilac Ujedinjenih nacija u svojoj zbirci „dobrih praksi" o obavještajnim službama i njihovom nadzoru[3] poziva na uvođenje postupaka za podnošenje „žalbi sudu ili nadzornoj instituciji, kao što je ombudsmen, povjerenik za ljudska prava ili državna institucija za ljudska prava" kada god neka osoba vjeruje da su njegova ili njena prava prekršena. Štaviše, žrtve nezakonitih radnji treba da „imaju mogućnost obraćanja instituciji koja im može pružiti učinkovit pravni lijek, uključujući punu naknadu za pretrpljenu štetu.[4] Ovo pravo na rješavanje slučajeva kršenja ljudskih prava utemeljeno je u međunarodnim zakonima o ljudskim pravima, koji također

zahtijevaju da osobe imaju pravo na učinkovit „pravni lijek."[5] Treba reći da „učinkovit lijek" u ovom kontekstu treba da bude više od obične naknade za utvrđeno kršenje prava. To uključuje i pravo na obraćanje instituciji koja može da presuđuje da li je pravo zaista bilo prekršeno ili nije.[6]

Izvještaj specijalnog izvjestioca dalje nalaže da institucije nadležne za rješavanje žalbi i zahtjeva za pravnim lijekom treba da budu nezavisne od obavještajnih službi i izvršne vlasti, te da „imaju puni i neometani pristup svim relevantnim informacijama, potrebna sredstva i stručnost da provode istrage, te pravo da izdaju obavezujuće naloge."[7]

Upravo ova posljednja pitanja forme predstavljaju i najkompleksnije izazove. Danas postoji prilično obiman korpus uporednih podataka koji se tiču oblika i veličine tijela za rješavanje žalbi u obavještajnom sektoru. Mada je sa resursima koji su nam na raspolaganju za ovaj projekat nemoguće ocijeniti kako stvarno rade ova tijela,izvjesni zaključci mogu se izvući iz strukture, opsega i ovlasti samih sistema. Očito je iz ovog pregleda da, dok je potreba za sistemom žalbe nužna, uspostava jednog učinkovitog sistema može biti prije umjetnost nego nauka. Države moraju odlučiti da li da se oslone na postojeće sudove ili da osnuju posebna tijela za rješavanje žalbi. Ako izaberu ovu drugu varijantu, države mogu kreirati posebne režime "rukovanja" informacijama kojim će riješiti probleme tajnosti i sigurnosti koje sobom nose žalbe vezane za obavještajne službe. U isto vrijeme, obraćanje specijaliziranim tijelima za rješavanje žalbi otvara druga pitanja, od kojih nisu najmanje važna pitanja nadležnosti, članstva i ovlasti da se odlučuje o pravnom lijeku.

Rečena pitanja se razmatraju dalje u tekstu tako što su grupirana u nekoliko cjelina: podnošenje žalbi; tijela za ulaganje žalbi; žalbena procedura i kontrola informacija; te pravni lijekovi u vezi sa žalbama.

2. PODNOŠENJE ŽALBI

Postojeća pravila utvrđuju ko je nadležan za podnošenje žalbi. Žalbe vezane za obavještajne službe mogu se podijeliti u dvije kategorije; prva, „insajderske" žalbe; i, druga, žalbe „javnosti". U svrhu ovog rada, „insajderske" žalbe su žalbe koje nezavisnom tijelu podnesu službenici obavještajne službe ili drugih vladinih službi, koji su pogođeni nekom radnjom obavještajne službe. „Javne" žalbe su žalbe koje podnose pripadnici javnosti koji nisu vezani za obavještajnu zajednicu, niti za vladu.

2.1 INSAJDERSKE ŽALBE

U nekim državama, službenici obavještajne službe ili drugih vladinih službi imaju mogućnost podnošenja žalbe protiv obavještajne službe. Te insajderske žalbe nekad su vezane za tretman podnosioca žalbe od strane obavještajne službe. Na primjer, u Kanadi, Kanadska sigurnosno-obavještajna služba (CSIS) obavlja gotovo sve istrage vezane za provjeru sigurnosti za Vladu Kanade, koje se rade u svrhu sigurnosne provjere vladinih službenika. Službenik koji nije zadovoljan rezultatom procesa sigurnosne provjere može se žaliti nezavisnom administrativnom tijelu (ili stručnom nadzornom tijelu), poznatom kao Sigurnosno-obavještajni odbor za ocjenu (SIRC).[8]

U drugom slučaju, "insajderske" žalbe mogu biti općenite i ukazivati na greške ili pretjerani angažman obavještajne službe. U Belgiji, na primjer, istražna služba Stalnog odbora za

ocjenu obavještajnih agencija (poznat kao Odbor I) ima ovlast da:

> *Razmotri žalbe i optužbe pojedinaca koje se direktno tiču intervencije neke obavještajne službe... Svaki državni službenik, svaka osoba koja obavlja javnu funkciju i svaki pripadnik oružanih snaga, kojih se direktno tiču direktive, odluke ili pravila, kao i metode ili radnje koje su na njih primjenjive, mogu podnijeti žalbu … a da pritom ne trebaju tražiti saglasnost svojih nadređenih.*[9]

Po zakonu Sjedinjenih Američkih Država, službenik CIA-e ili firma-ugovorač CIA-e mora provesti interni proces obavještavanja prije nego što podnese žalbu kongresnim odborima za nadzor. Važeći zakon također omogućava da insajder „koji namjerava Kongresu uložiti žalbu ili dostaviti informaciju u vezi sa nekim hitnim pitanjem može takvu žalbu ili informaciju podnijeti generalnom inspektoru."[10] "Hitno pitanje" u ovom kontekstu znači sljedeće:

- Ozbiljan ili flagrantan problem, zloupotrebu, kršenje zakona ili odluke izvršne vlasti, ili neki nedostatak vezan za finansiranje, upravljanje ili provođenje neke obavještajne aktivnosti koje se tiču klasificiranih informacija, ali ne isključuje razlike u mišljenjima koja se odnose na pitanja javne politike;
- Netačnu izjavu Kongresu, ili svjesno sakrivanje od Kongresa, oko pitanja koja se tiču materijalne činjenice vezane za finansiranje, upravljanje ili provođenje neke obavještajne aktivnosti.[11]

Insajderske žalbe ove vrste su jedan vid "zviždača" – njima se razotkrivanju greške izvan redovnog lanca komande u obavještajnim službama, a da se pritom obavezno ne otkrivaju tajne mimo uskog kruga vladinih agencija ili drugih ovlaštenih nadzornih tijela. Raspoloživost takvih žalbenih mehanizma može smanjiti vjerovatnoću da će neki uposlenik preduzeti ekstremnije oblike razotkrivanja, na primjer, odavanja medijima.

Sasvim razumljivo, neka pravna rešenja potiču na korištenje ovog oblika zviždača, nudeći, na primjer, zaštitu insajderu koji podnese žalbu putem ovih ovlaštenih kanala. Na Novom Zelandu, na primjer, „ukoliko uposlenik obavještajne ili sigurnosne agencije skrene pažnju generalnom inspektoru na neko pitanje [vezano za obavještajni rad i sigurnost], taj uposlenik neće biti izložen nikakvim kaznama niti diskriminatornom tretmanu od strane te obavještajne i sigurnosne agencije u vezi sa njegovim zaposlenjem samo zato što je skrenuo pažnju generalnom inspektoru na to pitanje", osim ako to uradi sa lošom namjerom.[12] U Sjedinjenim Državama, „nijednu radnju koja predstavlja odmazdu ili prijetnju odmazdom zbog podnošenja takve žalbe ne može preduzeti nijedan uposlenik [Centralne obavještajne] agencije, koji je u poziciji da preduzme takve radnje, osim ako je ta žalba podnesena, ili ta informacija data uz punu svijest da je lažna, ili sa svjesnim nemarom prema njenoj tačnosti ili netačnosti."[13]

U nekim državama, postojanje internih zviždača je preduslov za javne, vanjske oblike ove prakse. U Kanadi, na primjer, podnosilac žalbe koji propusti da na prekršaj upozori koristeći prvo unutrašnje mehanizme može imati poteškoća da se uspješno odbrani od krivičnih optužbi zbog neovlaštenog otkrivanja klasificiranih informacija.[14]

1.2 JAVNE ŽALBE

Javne žalbe su postupci koje pokreću osobe koje nisu povezane sa vladom. Te vrste žalbi imaju drugačiji osnov u odnosu na insajderske žalbe. S jedne strane, javni podnosioci

žalbi mogu biti tek nejasno svjesni grešaka o kojima se radi. Pripadnik javnosti koji je bio pogrešno praćen, na primjer, može za taj problem saznati tek slučajno, a čak i tada može biti nesvjestan tačnog identiteta agencije koja je vršila praćenje. Iz tih razloga, takva osoba će vjerovatno imati malo konkretnih informacija na kojima će zasnivati svoju žalbu. Također se može desiti da ta osoba dolazi iz društvene, etničke ili religijske grupe koja nije sklona, ili je se i inače odvraća od podnošenja žalbi. Klasičan primjer takve osobe može biti imigrant koji nije upoznat sa institucijama i praksama društva u koje je došao.

Svaki sistem javne žalbe mora, stoga, biti takav da umanji neizvjesnost te mora biti široko dostupan. To znači da treba da postoji širok osnov za javne žalbe i malo prepreka za pokretanje istraga kao reakcija na žalbe.

Neke države osiguravaju da ne postoje ograničenja u pogledu klase osobe koja ima pravo da podnese žalbe, te time što dozvoljavaju da se oni žale na veliki broj tema. U Holandiji, na primjer, nakon što se obavijesti nadležni ministar kako bi mu se omogućilo da iznese gledište, „svaka osoba“ može podnijeti žalbe državnoj instituciji ombudsmena u vezi sa provedbom važećeg zakona od strane obavještajnih službi.[15] U Irskoj, Komisija ombudsmena Garda Síochána može „primiti žalbe koje podnesu pripadnici javnosti a koje se odnose na ponašanje članova Garda Síochána” (tj. policije).[16] Slično, u Kanadi najopćenitija žalba koju javni podnosilac žalbe može podnijeti protiv sigurnosno-obavještajne službe tiče se “svakog akta ili stvari koju uradi Služba.”[17] Konačno, u Sjedinjenim Državama, Generalni inspektor CIA-e “ovlašten je da prima i istražuje žalbe ili informacije od bilo koje osobe u vezi sa postojanjem neke aktivnosti koja predstavlja kršenje zakona, pravila ili propisa, ili pogrešno upravljanje, neopravdano trošenje sredstava, zloupotrebu ovlasti, i specifičnu prijetnju za javno zdravlje i sigurnost.”[18]

Ove široke formulacije mogućnosti da javnost podnese žalbe čine se poželjnim ukoliko je svrha modela za rješavanje žalbi da bude “starija” od drugih sredstava reguliranja zakonitosti i ispravnosti ponašanja obavještajne službe. Ipak, u nekim se državama ne primjenjuju široki koncepti mogućnosti javnosti da podnese žalbu te se pravo na podnošenja žalbi ograničava na klasu pojedinaca koja je uža od koncepta „svaka osoba“. Neka od tih ograničenja čine se skromnim, ali mogu biti sasvim neizvjesna u svom osnovu. Na primjer, Kenijska žalbena komisija može primiti žalbe od „bilo koje osobe pogođene“ od strane obavještajne službe u provođenju njenih ovlasti ili obavljanju njenih funkcija.[19] U Južnoj Africi, „svaki pripadnik javnosti“ može podnijeti žalbu Zajedničkom stalnom odboru za obavještajni rad „u pogledu bilo čega za što pripadnik javnosti vjeruje da je služba izazvala njegovoj ili njenoj osobi ili imovini.”[20]

Čini se da oba ova pristupa onemogućavaju preemptivne ili spekulativne žalbe koje su potaknute pukom sviješću o određenoj praksi obavještajne službe. Na primjer, neko udruženje etničkih manjina koje sumnja da se u obavještajnim istraga vrši tzv. ”etničko profiliranje” (eng. ethnic profiling) možda neće imati pravo da podnese žalbu ukoliko ne postoji podnosilac žalbe sa ličnim iskustvom u vezi sa takvim praksama. Teško je utvrditi da ovakvo ograničavanje nudi bilo kakvu dodanu vrijednost, ako je svrha žalbenog sistema da regulira zakonitost i ispravnost rada obavještajnih službi.

Čak je problematičnije kada pravni režim zemlje nameću da podnosioci žalbe mogu biti samo državljani ili osobe sa stalnim boravištem. Tako, na primjer, generalni inspektor za obavještajni rad i sigurnost Novog Zelanda može primiti žalbu samo od „osobe sa Novog Zelanda“ (građanina ili osobe sa stalnim boravištem), ili osobe koja je bila, ili je trenutno

uposlena u jednoj od obavještajnih službi.[21] Australijski generalni inspektor za obavještajni rad i sigurnost (IGIS) može primiti jedino žalbe koje se tiču australijske vanjske obavještajne službe od „osobe koja je australijski državljanin ili ima stalno boravište u Australiji."[22] (Ova ograničenja u pogledu nacionalnosti se ne primjenjuju, međutim, u vezi sa žalbama koje se tiču domaće sigurnosno obavještajne službe Australije.)

Pravila o nacionalnosti (ili nacionalnosti/boravištu) su proizvoljna prepreka za podnošenje žalbe. Rezultat može biti sprječavanje da informacije dopru do ciljnih grupa koje su osobito vjerovatan predmet praćenja, uključujući osobe koje traže status izbjeglice i druge strance koji još nemaju stalno boravište, niti su dobili državljanstvo. I u tim slučajevima se može reći da, u mjeri u kojoj žalbe služe kao rano upozorenje na prekršaj, teško da postoji bilo kakva dodana vrijednost u ovakvom ograničavanju prava na podnošenje žalbe.

3. TIJELA ZA PODNOŠENJE ŽALBI

Ovo poglavlje bavi se tijelima kojima se žalba može podnijeti. Različite su institucije kojima se žalbe podnose. Generalno govoreći, te institucije mogu se podijeliti u dvije široke klase: opća tijela i specijalizirana tijela. Pod „općim tijelima", ovo poglavlje podrazumijeva instituciju *bez* specijaliziranog mandata za nadzor nad sigurnosnim ili obavještajnim službama. Primjeri općih tijela uključuju sudove, institucije ombudsmena, državne komisije za ljudska prava i druga regulatorna tijela, kao što su povjerenici za zaštitu podataka. "Specijalizirana tijela," s druge strane, su institucije sa specifičnim mandatom da se bave pitanjima sigurnosnih ili obavještajnih službi. Primjeri uključuju stručna nadzorna tijela kao što je Odbor I u Belgiji i SIRC u Kanadi.

3.1 OPĆA TIJELA

3.1.1. Redovni sudovi

U nekim državama, redovni građanski sudovi su nadležni da presuđuju po žalbama vezanim za obavještajne službe, utemeljenih kao prepoznatljivi oblici građanskopravnih grešaka (uključujući različite oblike prekršaja). U drugim, administrativni sudovi mogu presuđivati u predmetima u okviru njihove vlastite predmetne nadležnosti (npr, upravni zakon) koje se tiču radnji obavještajnih službi.[23]

Zapravo, barem u nekim država, određeni sudovi predstavljaju jedina tijela nadležna za primanje žalbi vezanih za obavještajne službe.[24] Ne postoje specijalizirana tijela za nadzor obavještajnih službi koja su ovlaštena da primaju žalbe. Takav izbor krije razne izazove. Kao što u daljem tekstu razmatramo, sudovi mogu biti nadležni da dodijele jak pravni lijek, ali iz praktičnih razloga također može biti gotovo nemoguće da podnosilac žalbe dobije takav pravni lijek: nekad se tako jedinstvene žalbe na obavještajne službe "guraju" pod konvencionalnu nadležnost redovnih sudova (npr., kao prekršaj za koji se može pokrenuti građanskopravni postupak) ili se uopće ne rješavaju na sudovima.

3.1.2. Konvencionalna regulatorna tijela

Važno je također da, poput drugih vladinih institucija, obavještajne službe potpadaju pod nadležnosti institucija koje imaju opći mandat da rješavaju žalbe o javnim tijelima

ili mandat da se bave određenim predmetima koji nisu specifični za obavještajne službe. Te institucije uključuju institucije obudsmena, komisije za zaštitu podataka, i komisije za ljudska prava. One mogu, na primjer, biti nadležne da postupaju po žalbama koje se odnose na korištenje informacija obavještajnih službi ili, općenito, na njihovo poštivanje ljudskih prava. U Holandiji, na primjer, žalbe mogu biti podnesene državnom ombudsmenu o radnjama, između ostalog, nadležnog ministara, šefova Generalne obavještajne i sigurnosne službe ili Odbrambene obavještajne i sigurnosne službe i osoba koje rade za ta tijela.[25] Slično, u Finskoj i Švedskoj, žalbe koje se tiču sigurnosne policije mogu se podnijeti instituciji parlamentarnog ombudsmena.[26] U Belgiji, Finskoj i Kanadi, komesar za privatnost (ili zaštitu podataka) može primati žalbe koje se tiču tretmana ličnih informacija od strane obavještajnih službi.[27]

U nekim državama, regulatorna tijela koja su zadužena za određene oblasti treba po zakonu da konsultuju specijalizirana tijela za nadzor nad obavještajnim službama ili tijela za rješavanje žalbi (koja su tema sljedećeg poglavlja), ako se žalba tiče obavještajnih službi i/ili pitanja državne sigurnosti. U Kanadi, na primjer, Komisija za ljudska prava mora SIRC-u uputiti žalbu u vezi sa praksom "koja se odnosi na pitanja vezana za sigurnost u Kanadi". SIRC potom istražuje slučaj i podnosi izvještaj Komisiji, koja odlučuje da li da pokrene postupak po žalbi.[28] Ovakva podjela nadležnosti neizbježno komplicira predmete, ali zato omogućava da manji krug osoba rukuje klasificiranim informacijama. Stoga je manje vjerovatno da će rješavanje žalbi biti onemogućeno zbog nespremnosti obavještajnih službi da svoje klasificirane informacije podijele sa konvencionalnim regulatornim tijelima.

3.1.3. Nedostaci općih tijela za podnošenje žalbi

Ono što općenito brine u vezi sa općim tipom tijela za podnošenje žalbi – bilo da su to sudovi ili konvencionalna regulatorna tijela – jest pristup klasificiranim informacijama. U nekim državama, građanski sud može imati ovlast da u slučaju da oštećeni koji uspiju dokazati da su bili u pravu donesu presudu o naknadi štete, u slučaju da su obavještajne službe počinile građanskopravni prekršaj. Međutim, u praksi se ovakvi predmeti na redovnom sudu teže dobijaju zbog zahtjeva vlade za čuvanjem tajne. Pošto podnosilac tužbe snosi teret dokazivanja, kontrola nad relevantnim činjenicama od strane vlade može gotovo onemogućiti uspjeh u građansko-pravnom predmetu.[29] Jednako tako, konvencionalna regulatorna tijela nisu specifično zadužena za obavještajna pitanja i pitanja državne sigurnosti te se može desiti da nisu u mogućnosti da pristupe i provjeravaju klasificirane informacije prilikom istraga po žalbama vezanim za obavještajne službe. Na primjer, opće tijelo za rješavanje javnih žalbi zaduženo za kanadske državne policijske snage, Kanadsku kraljevsku konjičku policiju, nekoliko se puta žalilo da nije u stanju ispitati policijske aktivnosti vezane za državnu sigurnost zbog njihove tajnosti.[30]

Može se također desiti da su opća tijela za podnošenje žalbi previše opća, tj. da nemaju stručno znanje za bavljenje sigurnosnim i obavještajnim službama. Konsekvenca tog nedostatka je da su opća tijela sklonija da prihvate zahtjeve za čuvanje tajne ili druge oblike specijalnih okolnosti koje podnose obavještajne službe, nego što je to slučaj sa stručnim nadzornim tijelima sa dugim iskustvom u nadziranju takvih službi.

Na kraju, sama priroda žalbi koje se ulažu na račun obavještajnih službi može dovesti do toga da konvencionalni sudovi i regulatorna tijela ne budu osposobljena za njihovo rješavanje. Podnosioci žalbe su često obavezni da svoje pojedinačne žalbe u pogledu zakonitosti ili ispravnosti ponašanja uklapaju u standardne građanskopravne i regulatorne

osnove za podnošenje žalbe. Pošto je nekad teško uklopiti se, te meritorne žalbe mogu biti odbačene ne zato što ne otvaraju ozbiljne sumnje u pogledu sigurnosne službe, već zato što te sumnje ne mogu biti iskazane pravnim jezikom općeg tijela za rješavanje žalbi. Nezakonito tajno praćenje, na primjer, u nekim državama može biti teško prepoznati kao građanskopravni prekršaj, te se stoga može desiti da ne potpadne pod nadležnost redovnih sudova.

3.2 SPECIJALIZIRANA TIJELA ZA PODNOŠENJE ŽALBI

Jedan očiti odgovor na nedostatke općih tijela jeste osnivanje specijaliziranih tijela za rješavanje žalbi. Specijalizirani tijela obično se uklapaju u jednu od tri kategorije: prvo, mogu biti dio izvršne grane vlasti (npr. generalni inspektor); drugo, mogu biti nezavisni od izvršne grane vlasti i parlamenta; i, konačno, mogu biti parlamentarna tijela.

3.2.1 Interna tijela za rješavanje žalbi

Neke države imaju unutarnja nadzorna tijela, koja služe kao sredstva izvršne vlasti za nadzor nad obavještajnim službama. Ta tijela mogu jednostavno biti ministar ili specijalni predstavnik ministra, obično u zvanju generalnog inspektora. Treba zapaziti, međutim, da je u nekim zemljama generalni inspektor istinski nezavisno tijelo – to jest, on ili ona ima sigurnost mandata i nezavisnost u djelovanju, što inspektora stavlja izvan komande i kontrole izvršne vlasti i obavještajnih službi. U nekim slučajevima, interna tijela mogu biti nadležna da primaju javne žalbe.[31] Iz perspektive izvršne vlasti, takav pristup umanjuje potrebu da se klasificirane informacije, koje mogu biti predmet žalbe, otkriju izvan vrlo uskog kruga osoba. Međutim, interna tijela za rješavanje žalbi nemaju nezavisnost i autonomiju od onih koji su odgovorni za upravljanje obavještajnim službama. Javnost može ta tijela doživljavati kao tijela podložna sukobu interesa koji proizlazi iz činjenice da „lisica čuva kokošinjac“, što može izazvati sumnje u legitimnost internog procesa rješavanja žalbi.

3.2.2 Nezavisna tijela za rješavanje žalbi

Struktura

Nezavisnija, ali još uvijek usko specijalizirana, tijela za rješavanje žalbi predstavljaju očiti kompromis između potrebe da se ograniči diseminacija klasificiranih informacija i istovremeno ojača javni legitimitet. Jedan broj zemalja uspostavio je stručna nadzorna tijela koja imaju vlastite službenike i rade nezavisno od obavještajnih službi i ostatka izvršne grane vlasti. Te agencije uživaju kredibilitet koji proizlazi iz njihovog nezavisnog rada. Ipak, ta tijela mogu biti dovoljno bliska vladi da bi njihovi uposlenici mogli biti sigurnosno provjereni kako bi im se moglo povjeriti klasificirane informacije. To je upravo praksa propisana u zakonu koja važi za jedno od prvih takvih tijela, kanadski SIRC, koje je stvoreno u nastojanju da se ublaži zabrinutost obavještajne službe u pogledu protoka klasificiranih informacija. Pripadnike SIRC-a imenuje savezna izvršna vlast, ali nakon konsultacija sa opozicijskim partijama u parlamentu. Njegovi pripadnici uživaju znatnu sigurnost mandata, koji je obnovljiv na pet godina, te mogu zaposliti vlastite službenike, mada uz saglasnost dijela izvršne vlasti koji upravlja finansijama. Svaki član zaklinje se na čuvanje tajne te je podložan kanadskom Zakonu o državnoj tajni.[32]

Dok kanadski sistem ne obavezuje na imenovanje pojedinaca sa posebnim stručnim znanjem, druge zemlje primjenjuju drugačiji pristup. Na primjer, Komisija za žalbe

Kenijske obavještajne službe na čelu ima sudiju, a čine je još četiri člana, od kojih je jedan „advokat“ koji ima više od sedam godina radnog iskustva, a jedan mora biti „vjerski lider“ od „nacionalnog ugleda“. Članove komisije imenuje predsjednik, „po savjetu Komisije za pravosuđe“ na „trogodišnja mandat“, koji se može ponoviti maksimalno dva puta.[33] S druge strane, belgijski Odbor I imenuje Senat na obnovljivi šestogodišnji mandat, a njegovi članovi moraju ispunjavati određene kvalifikacijske kriterije u pogledu poznavanja prava i relevantnog iskustva, te ne smiju biti pripadnici policije ili obavještajne službe.[34]

Teško je sa distance procijeniti koliko takvi nezavisni sistemi imenovanja zaista ispunjavaju svoju svrhu u praksi. Međutim, sam princip je dosta dobar. Štaviše, sistemi imenovanja koji nameću kompetentnost i profesionalno iskustvo su sigurni, ako to nema utjecaja na stvaranje ekskluzivne kaste osoba sa pravom da budu imenovane. Jako uski i zahtjevni kriteriji za imenovanje mogu krug osoba koje ispunjavaju uslove svesti samo na one koji su nekad radili u obavještajnoj službi – što bi vodilo percepciji (čak ako tako nije u stvarnosti) da nadzorno tijelo drži u rukama obavještajna služba koju ono nadzire.

Tribunal sa istražnim ovlastima Ujedinjenog Kraljevstva predstavlja primjer sasvim drugačijeg seta profesionalnih očekivanja: njegovi članovi su isključivo osobe koje su bile na visokom položaju u pravosuđu ili su se bar deset godina bavile advokaturom.[35] Ipak, članstvo koje čine samo advokati i bivše sudije može također biti ekstremno. Ima izvjesnih prednosti ukoliko sastav tijela koje služi širokom javnom interesu odražava različite perspektive i različita profesionalna iskustva.

To je filozofija koja, čini se, stoji iza kanadskog SIRC-a: nema profesionalnih preduslova za članstvo. Umjesto toga, njegovi članovi moraju jednostavno biti članovi Državnog vijeća (Privy Council) Kanade koji nisu trenutno u saveznoj zakonodavnoj vlasti. U praksi, skup mogućih kandidata uključuje bivše visoke političare, vodeće sudije i „istaknute“ pojedince koji se ističu svojom čašću. Potpuno je moguće da osoba bude imenovana u Državno vijeće upravo zato da bi potom postala član SIRC-a. Drugim riječima, članstvo u SIRC-u je široko otvoreno što omogućava tom tijelu (barem principijelno) da predstavlja širu javnost kojoj i služi.

Fleksibilnost kanadskog pristupa može, međutim, otići predaleko. Neiskrenim se čini pristup po kojem se tijelo koje rješava žalbe, a koje ima kvazisudsku funkciju, potpuno prepusti u nadležnost osoba bez pravne kvalifikacije, što se može desiti kada je kanadski SIRC u pitanju. Koje god druge kvalitete članovi imaju, nedostatak pravnih kvalifikacija može dovesti do ovisnosti o pravnim službenicima koji rade u tijelu za rješavanje žalbi. To je slučaj koji, zauzvrat, zahtijeva pažljivu procjenu karijere tih pravnika i njihovo kretanje između i unutar vladinih tijela (uključujući, potencijalno, i obavještajne službe). Nezavisnost tijela za rješavanje žalbi može biti umanjena (ili se barem može tako doživjeti) kada su članovi ovisni o državnim službenicima koji s vremena na vrijeme rade u izvršnoj vlasti. S obzirom na to, idealni model mogao bi biti višečlano tijelo za rješavanje žalbi u čijem sastavu su osobe različitog zanimanja, pri čemu se mora osigurati da minimalna kvota tih članova ima, recimo, pravno znanje.

Funkcija

Neke države uspostavile su nadzorna tijela čija je jedina funkcija primati i istraživati žalbe. Na primjer, u Ujedinjenom Kraljevstvu, Tribunal sa istražnim ovlastima „može istraživati žalbe o bilo kojem navodnom ponašanju od strane ili u ime Obavještajnih službi - Sigurnosne

službe (poznate kao MI5), Tajne obavještajne službe (poznate kao MI6) i Vladinog centra za komunikacije (GCHQ).”[36]

U drugim slučajevima, glavna funkcija ovih stručnih nadzornih tijela je ocjena rada obavještajnih službi, bilo nezavisna, bilo po nalogu ministara ili parlamentaraca.[37] Međutim, ova tijela mogu također imati ovlaštenje da dobivaju (i istražuju) žalbe koje se tiču obavještajnih službi za koje imaju mandat nadzora.[38] U Norveškoj, na primjer, Parlamentarni odbor za nadzor obavještajnih službi je tijelo čiji članovi, mada ih bira parlament, nisu dio zakonodavne grane vlasti. Uz istrage aktivnosti obavještajnih službi na vlastitu inicijativu, ovaj odbor može također dobivati i istraživati žalbe od pripadnika javnosti.[39] Slično, belgijski Odbor I „bavi se žalbama i prijavama koje dobije u pogledu rada, djelovanja ili nedjelovanja obavještajnih službi, Koordinacijske jedinice za procjenu prijetnji, i drugih službi i njihovih službenika kojima pružaju podršku.”[40] Slične funkcije obavlja generalni inspektor obavještajne službe (IGI) Južne Afrike – ured koji je nezavisan od izvršne vlasti, a odgovoran parlamentarnom odboru za nadzor, koji se spominje u daljem tekstu. Generalni inspektor može „dobivati i istraživati žalbe od pripadnika javnosti i službi o navodnom pogrešnom upravljanju, zloupotrebi ovlasti; kršenjima Ustava, zakona i politika [koji se odnose na obavještajne i kontraobavještajne službe], korupciji i neopravdanom bogaćenju bilo koje osobe putem djelovanja ili propuštanja da djeluje bilo kojeg člana.”[41]

U nekim državama, prije žalbe koja se upućuje ovim stručnim nadzornim tijelima treba se obavijestiti obavještajna služba. U Kanadi, na primjer, javna žalba mora biti upućena prvo direktoru CSIS-a. SIRC može onda istražiti ozbiljne žalbe, podnesene u dobroj namjeri ako direktor ne odgovori u vremenskom periodu koji odbor smatra razumnim, ili ako da neadekvatan odgovor.[42]

3.2.3 Parlamentarna tijela za rješavanje žalbi

Jedan broj zemalja ima specijalna parlamentarna tijela koja nadziru obavještajni rad i te službe. Kao što se to odnosi na neka stručna gore navedena nadzorna tijela, ovi parlamentarni odbori mogu također imati odobrenje da dobivaju i istražuju žalbe koje se tiču aktivnosti obavještajne službe.[43] U Njemačkoj, na primjer, parlamentarni panel za kontrolu može primati žalbe.[44] U Južnoj Africi, parlamentarni Stalni zajednički odbor za obavještajne službe (tijelo kojeg čini petnaest članova parlamenta i koje ima funkciju nadzora nad obavještajnom službom) ne istražuje žalbe direktno već može:

> *narediti istragu te dobiti izvještaj od šefa službe ili generalnog inspektora u vezi sa bilo kojom žalbom koju Odbor dobije od bilo kojeg pripadnika javnosti, a u vezi sa bilo čime za za što taj pripadnik javnosti vjeruje da je Služba izazvala njegovoj ili njenoj osobi ili imovini: pod uslovom da Odbor utvrdi da takva žalba nije neozbiljna, ili provokativna, ili podnesena s lošom namjerom.*[45]

Ovlaštenje dato parlamentarnim odborima da vrše i funkciju nadzora i funkciju rješavanja žalbi omogućava koncentraciju stručnog znanja o sigurnosnom sektoru u jednom jedinstvenom tijelu, dok istovremeno ograničava diseminaciju klasificiranih informacija. Tu postoji, međutim, cijeli niz nedostataka vezanih za činjenicu da se parlamentarnim nadzornim tijelima prepušta da vrše funkciju rješavanja žalbi. Prvo, parlamentarci možda nemaju dovoljno stručnog znanja, ni vremena da istražuju i presuđuju po žalbama. Drugo, parlamentarci su, po definiciji, partijski akteri. To može kompromitirati njihovu sposobnost da istražuju i presuđuju na propisan način žalbe koje podrazumijevaju

posebno akutnu osjetljivost u pogledu vladanja aktualne vlade. Treće, rješavanje žalbi može zahtijevati pažljivu kontrolu zapisnika, poslovnika, te dokaza koji se tiču, na primjer, vjerodostojnosti svjedoka, što se bolje rješava u jednom više kvazisudskom okruženju. Konačno, parlamentarni odbori često imaju mnogo članova, što može otežati postizanje i uobličavanje jasnih presuda.

4. PROCEDURE RJEŠAVANJA ŽALBI I KONTROLA INFORMACIJA

Nije moguće u ovom kratkom poglavlju detaljno opisati procedure rješavanja žalbi. Fokus će stoga biti na nekoliko općih aspekata, kao i procedura koje se koriste za zaštitu klasificiranih informacija. Pošto su procedure koje provode tijela sa općijim mandatom (npr., mandatom da nadziru veći broj aktera, a ne samo obavještajne službe) veoma različite, fokus u ovom dijelu je na procedurama koje provode specijalizirana (za obavještajna i pitanja državne sigurnost) tijela za rješavanje žalbi o kojima je bilo riječi u prethodnom dijelu 3.2.

4.1 OPĆA PROCEDURALNA PRAVILA

Zakon u nekim državama zahtijeva da se žalbe moraju dostaviti napismeno.[46] Tijela za rješavanje žalbi mogu biti ovlaštena da odbace žalbe za koje procijene da su neozbiljne, zlonamjerne, podnesene sa lošom namjerom, ili potpadaju ispod praga (*de minimis*) za pokretanje istrage.[47] Takvo ograničenje očito umanjuje učinak široko postavljenih pravila, jer omogućava tijelu da odbaci žalbe koje očigledno nisu meritorne. Naravno, ako se primjenjuje preširoko kako bi se zaobišli teški predmeti, takva pravila mogu učiniti da tijelo za rješavanje žalbi bude neučinkovito u vršenju funkcije nadzora i rješavanja žalbi. U krajnjoj instanci, garancija za propisno korištenje ovih filter-pravila leži u nezavisnosti samog tijela. Ako su mu službenici pažljive i kvalificirane osobe dovoljno autonomne u odnosu na vladu, onda će oni imati malo poticaja da odbacuju kontroverzne predmete na čisto proceduralnim osnovama.

Veoma je važno da tijela za rješavanje žalbi ne miješaju žalbe koje su „neozbiljne i zlonamjerne“ sa onima koje „nisu potkrijepljene sa dovoljno detalja“. Kao što smo već rekli, od žalbi koje osporavaju ponašanje tajnovitih obavještajnih službi moglo bi se sa razlogom očekivati da ne sadrže mnogo detalja vezanih za otvorenije postupke. Isto tako, osnov „loše namjere“ za odbijanje ne smije se koristiti jednostavno kao odgovor na podnosioce žalbi koji su ”teške” osobe. Podnošenje žalbe protiv moćne obavještajne službe je teško te je vjerovatno da će samo najtvrdoglaviji posegnuti za tim. Podnosioci žalbe – a pogotovo zviždači – mogu imati drugačije osobenosti i vrijednosti od uobičajenih, te zbog toga mogu dovesti do toga da se legitimnost njihove žalbe dovode u pitanje. Posebnu pažnju treba posvetiti odvajanju činjenica od kvaliteta ličnosti koje mogu otvoriti prostor sumnji u vjerodostojnost.

Tamo gdje se vrše saslušanja ili istrage, važeća pravila barem nekih tijela za rješavanje žalbi nameću standarde pravednosti postupka, koji, na primjer, zahtijevaju da pogođene strane budu saslušane prije nego što se utvrde nalazi o neprihvatljivom ponašanju tih osoba.[48]

4.2 OVLASTI TIJELA ZA RJEŠAVANJE ŽALBI

Neka tijela za rješavanje žalbi imaju ovlasti da nalože izdavanje dokumenata i prisustvo

svjedoka.[49] Takve ovlasti mogu u nekim slučajevima biti jako široke i mogu zamijeniti, na primjer, privilegije odnosa advokat – klijent.[50] Na primjer, SIRC može imati pristup svim informacijama u posjedu obavještajne službe, isključujući vladine povjerljive dokumente (u biti to su zapisnici sjednica vlade). Drugdje, recimo, u Sjedinjenim Državama, generalni inspektor CIA-e

> *ima pristup bilo kojem uposleniku agencije ili bilo kojem uposleniku ugovarača agencije čije svjedočenje je potrebno radi obavljanja njegovih dužnosti. Usto, on će imati pristup svim evidencijama... koje se odnose na programe i operacije u vezi s kojim generalni inspektor ima odgovornost... Ukoliko bilo koji uposlenik ili ugovarač ne sarađuje sa generalnim inspektorom, to će se smatrati osnovom za odgovarajuće administrativne radnje koje pokreće direktor, a koje uključuju gubitak zaposlenja ili otkazivanje postojećeg ugovornog odnosa.*[51]

Za druga tijela za rješavanje žalbi, pristup informacijama je više zaobilazan. U Južnoj Africi, zakon zabranjuje parlamentarnom Stalnom zajedničkom odboru za obavještajne službe da ima pristup informacijama koje bi mogle otkriti identitet doušnika obavještajne službe.[52] S druge strane, IGI u Južnoj Africi uz manja ograničenja – „ni na koji način se ne može spriječiti da generalni inspektor pristupi obavještajnoj službi, informacijama ili prostorijama [sigurnosne službe].”[53] Ograničenje pristupa tajnim informacijama tijelu za rješavanje žalbi predstavlja očiti pokušaj da se ograniče mogućnosti svjesnog ili nesvjesnog curenja informacija. Ipak, ograničenja mogu onemogućiti tijelo za rješavanje žalbi da u potpunosti procjenjuje meritum žalbe. Drugim riječima, to može od samog početka biti hendikep za tijelo za rješavanje žalbi. Zato ovo može brinuti ako se namjerava stvoriti učinkovito tijelo za rješavanje žalbi.

Djelimično rješenje zbrci informacijske sigurnosti je propisati očekivanja u pogledu rukovanja informacijama u poslovniku tijela za rješavanje žalbi.[54] Južnoafrički IGI, na primjer, mora „ispuniti sve sigurnosne zahtjeve primjenjive na službenike obavještajne službe.”[55] U Kanadi, članove SIRC-a obavezuje kanadski Zakon o državnoj tajni te su stoga podložni krivičnom gonjenju, ukoliko pogriješe i otkriju tajne informacije.[56]

Postoje također protokoli radi fizičkog toka informacija. Na primjer, uposlenici SIRC-a obično pregledaju klasificirane informacije u bezbijednim uredima SIRC-a koji se zapravo nalaze u CSIS-ovim objektima. Dešavaju se slučajevi, međutim, kada se informacija iz SIRC-ovih vlastitih bezbijednih prostorija premješta, što se nerijetko dešava kada po informacijama navedenim u žalbi presuđuje SIRC. Stvaranje te infrastrukture za rukovanje informacijama može zahtijevati znatnu investiciju, a u geografski velikoj zemlji (poput Kanade), može ograničiti mjesta na kojima će SIRC provoditi svoje postupke.

4.3 POVJERLJIVOST U POGLEDU DRŽAVNE SIGURNOSTI

Kao što ranija diskusija sugerira, profesionalno rukovanje informacijama koje se tiču državne sigurnosti je ključna preokupacija svakog sistema rješavanja žalbi. Zakoni o mnogim tijelima za rješavanje žalbi posebno navode da istrage i/ili saslušanja moraju biti provedena iza zatvorenih vrata.[57] Usto, nalazi tijela za rješavanje žalbi mogu biti podložni redakturi i/ili njihova diseminacija može biti ograničena. Na primjer, u Australiji, IGIS ne smije dati svoje nalaze podnosiocu žalbe „sve dok se šef odnosne [obavještajne] agencije i Generalni inspektor ne saglase da davanje odgovora podnosiocu žalbe neće ugroziti sigurnost i odbranu Australije, ili odnose Australije sa drugim zemljama.”[58] U Južnoj Africi

također, IGI ne može objaviti povjerljive informacije bez prethodne dozvole vlade.[59] Slično tome, u Keniji, Žalbena komisija mora „poštovati zahtjeve državne sigurnosti“ u vršenju svojih funkcija. U tom cilju, ona mora konsultirati generalnog direktora Državne sigurnosno–obavještajne službe (i Vijeće za državnu sigurnost na ministarskom nivou) “u utvrđivanju informacija i okolnosti pod kojima određena informacija ne može biti objavljena tokom ili u vezi sa bilo kojom istragom u interesu državne sigurnosti.”[60] U Norveškoj, izjave Odbora podnosiocima žalbi „trebaju da budu onoliko potpune koliko je to moguće bez otkrivanja klasificiranih informacija.”[61]

Pošto tajnost može spriječiti podnosioca žalbe da uspješno podnese žalbu, neke države, kako bi se pomoglo podnosiocu žalbe, mogu primijeniti posebne procedure u zatvorenim dijelovima saslušanja. U Kanadi, na primjer, Vijeće SIRC-a ima ovlasti da

> *ospori odluke o neotkrivanju informacije sadržane u zatvorenom materijalu, kao i unakrsno ispitivanje vladinog svjedoka u zatvorenim postupcima. … Vanjski savjeti (ili ‘pravni zastupnici) mogu se zadržati u nekim slučajevima gdje zbog pitanja obima posla, unutarnji savjetnici nisu potpuno sposobni da postupaju u adversarnom sudskom postupku. U drugim slučajevima, pravni zastupnici mogu biti zadržani kada unutrašnji zastupnici procijene da slučaj zahtijeva posebno agresivno unakrsno ispitivanje od strane CSIS-a.*[62]

5. PRAVNI LIJEKOVI

Kao što je gore navedeno, ključna svrha bilo kojeg žalbenog sistema je „učinkovit pravni lijek“. Treba reći da pravni lijekovi koje nude tijela za rješavanje žalbi obavještajnih službi često predstavljaju preporuke, a ne obavezujuće pravne odluke koje se odnose na, na primjer, naknadu štete.[63] Ta ograničena ovlaštenja vjerovatno odražavaju dvojni mandat mnogih tijela za rješavanje žalbi; to jest, tijelo koje prima žalbe je jedno te isto tijelo kao i ono koje provodi autonomni nadzor aktivnosti obavještajnih službi. Ti procesi nadzora obično generiraju preporuke datoj obavještajnoj službi i izvršnoj grani vlasti u pogledu reformiranja politika i praksi. U slučajevima gdje je nadzor primarna funkcija tijela za rješavanje žalbi, zakonodavci koji su osnovali te institucije vjerovatno su smatrali da mogućnost da im se da ovlast da donose odluke o naknadi štete kao odgovor na žalbe nije u skladu sa činjenicom da učinkovit nadzor podrazumijeva postupak koji nije do te mjere adversaran.

U praksi, međutim, ograničavanje tijela za rješavanje žalbi da daju preporuke može ograničiti njihovu sposobnost da učine više nego da osramote obavještajnu službu te je tako navedu da poštuje propise. Ovaj pristup može biti posebno težak tamo gdje se rezultati istraga po žalbama i sami tretiraju kao klasificirana informacija, što je česta praksa o kojoj smo već govorili. Iz tog razloga, ima logike u stavu da tijela za rješavanje žalbi daju samo prerađene verzije svojih nalaza u svojim godišnjim izvještajima koji su dostupni javnosti ili na drugi način. Čak i ovi, međutim, mogu privući iznenađujuće malo pažnje parlamentaraca i medija. Kanadski SIRC, na primjer, objavio je sažetke nekad veoma osuđujućih nalaza koji su, međutim, izazvali jako malo trajnog interesa.

U najgorim slučajevima, puka ovlast da se daju preporuke može uticati na smanjenje svih drugih prednosti koje tijelo za rješavanje žalbi inače ima. Ako potencijalni podnosioci žalbe sumnjaju da će njihove radnje rezultirati bitnom reakcijom, promjenom ili naknadom,

oni mogu imati malo razloga da podnose žalbu tijelu za rješavanje žalbi. Prema tome, podnosioci žalbe mogu pokušati da svoje nezadovoljstvo rješavaju drugim kanalima (poput običnih sudova koji inače nisu u poziciji da na pravi način rješavaju te žalbe), da ih otkriju medijima u nadi da će to podstaći reakciju ili jednostavno neće htjeti ulagati bilo kakav napor oko toga. Svi ti odgovori podrivaju sam razlog postojanja tijela za rješavanje žalbi – da razotkriju i odgovore na prekršaje obavještajnih službi.

Druga tijela imaju više „sudske" ovlasti. To se posebno odnosi na tijela za rješavanje žalbi kojima je rješavanje žalbi jedini zadatak. Tako, kvazisudska tijela, kao što je Tribunal sa istražnim ovlastima u Ujedinjenom Kraljevstvu, imaju ovlast da nemetnu „mjere u smislu pravnog lijeka, kao što je ukidanje bilo kakvih naloga, uništenje bilo kakve evidencije koja se drži ili finansijsku naknadu."[64]

6. PREPORUKE

Jedan broj preporuka proističe iz prethodnog pregleda tijela za rješavanje žalbi. One su sumirane u diskusiji koja slijedi i predlažu se kao „najbolje prakse" u Tabeli 1.

- Države treba da formiraju tijela za rješavanje žalbi sa zadatkom primanja i istrage kako insajderskih tako i javnih žalbi.

Sistemi za rješavanje insajderskih žalbi predstavljaju sredstvo za usmjeravanje „zviždača" na institucionalni okvir koji reagira na meritorne žalbe i istovremeno rješava problem zabrinutosti vlade u pogledu zaštite klasificiranih informacija. Međutim, ovaj sistem treba također da proširi zaštitu na one koji ga primjenjuju.

- Učinkovit sistem insajderskih žalbi treba da uključi garancije da neće biti odmazde u slučajevima kad uposlenici sa dobrom namjerom podnesu žalbe ovlaštenim tijelima.

Sistemi javnih žalbi, nasuprot tome, su širi i općenito otvoreni za sve osobe. Malo zemalja nameće uslov da podnosilac žalbe može biti samo državljanin te države, i to uglavnom samo u vezi sa operacijama u inostranstvu. A čak još manje njih zahtijeva da je podnosilac žalbe lično pogođen na neki način u vezi sa predmetom na koji se odnosi žalba. Teško je vidjeti bilo kakvu stvarnu vrijednost u ograničenju mogućnosti podnošenja žalbe na takav način.

- Tijela za podnošenje žalbi treba da imaju široke nadležnosti kako bi primali žalbe od javnosti.

Široko postavljena pravila u odnosu na to ko ima pravo podnijeti žalbu znači da će se tijelu za rješavanje žalbi dostavljati više žalbi. Takva pravila također povećavaju količinu posla za ta tijela. Možda bi bilo ispravno ograničiti te slučajeve samo na one koji imaju meritum. Ali, dužnu pažnju treba posvetiti načinu na koji se meritum utvrđuje.

- Pitanja vezana za neozbiljne ili zlonamjerne žalbe mogu se rješavati pravilima koja omogućavaju tijelu za rješavanje žalbi da odbaci takve žalbe već na početku samog procesa. Ali treba biti jako oprezan kako bi se izbjeglo odbacivanje žalbi koje su teške, politički kontraverzne ili prosto ih podnose „teške" osobe.

U pogledu tijela kojima se upućuju žalbe, države treba pažljivo da razmotre da li su sudovi opšte nadležnosti ili konvencionalna regulatorna tijela adekvatno osposobljena da rješavaju žalbe vezane za obavještajne službe. U praksi, ta tijela su u nemogućnosti da se bave klasificiranim materijalom koji se tiče državne sigurnosti i/ili obavještajnih službi, što rezultira time da njihova učinkovitost bude umanjena, ili da, pak, ne mogu da adekvatno istraže žalbe. Nadalje, može se desiti da ta opća tijela nemaju stručno znanje vezano za predmet, a koje je potrebno da se podrobno istraže takva pitanja.

Poređenja radi, tijela za rješavanje žalbi koja su specijalizirana za obavještajne službe mogu biti strukturirana tako da odgovore na zabrinutost zbog pitanja zaštite klasificiranih informacija. Istovremeno, pitanja tajnosti podataka ne smiju imati utjecaja na umanjivanja funkcija specijaliziranog tijela za rješavanje žalbi do te mjere da ona ne mogu obavljati svoj glavni zadatak – rješavanje žalbi. Transparentnost treba da bude zajamčena, pri čemu se tajnost treba ograničiti na *bona fide* okolnosti. Više od toga, treba da se čine napori da se osigura izvjestan paritet između kapaciteta vlade i podnosioca žalbi da iznesu svoje argumente. Tamo gdje vlada može maskirati svoj stav krijući se iza tajnosti, tijelo za rješavanje žalbi treba da podrobno ispita taj slučaj. Nadalje, članovi nadzornih tijela treba da prođu sigurnosne provjere,kako bi imali široki pristup informacijama u posjedu vlade ili obavještajnih službi.

- U većini slučajeva, specijalizirana tijela za rješavanje žalbi treba da imaju prednost nad općim pristupom rješavanja žalbi kada se radi o istraživanju žalbi vezanih za obavještajne službe. Takva tijela treba da imaju široke ovlasti u pogledu pristupa klasificiranim informacijama, a od njih treba obavezati na čuvanje povjerljivih informacija kako bi smanjile mogućnosti da te informacije neovlašteno procure (namjerno ili nenamjerno). To se može učiniti putem specijalnih protokola o rukovanju informacijama i afirmativnim obavezama u pogledu sigurnosne provjere.

Tijela za rješavanje žalbi će biti vjerodostojna samo kada imaju uposlenike i kada rade nezavisno od vlade, te kada su na odgovarajući način opremljena. Dok tijela za rješavanje žalbi u svom sastavu ne smiju imati samo one sa posebnom profesionalnom usmjerenošću (npr., pravnike), mora postojati adekvatna zastupljenost pravnika u njihovom članstvu. Nezavisna pravna kompetentnost smanjuje rizik onoga što bi inače moglo biti pretjerana ovisnost o pravno kvalificiranim (možda ne tako nezavisnim) članovima osoblja.

- Tijela za rješavanje žalbi moraju biti nezavisna u odnosu na vladu. U praksi, to znači da se imenuju na način koji ne predstavlja unilateralno imenovanje od strane aktualne vlade i da su oni slobodni da djeluju autonomno od vlade, dok istovremeno imaju siguran mandat. Barem neki članovi treba da imaju pravničke kvalifikacije kako bi se izbjegla pretjerana ovisnost o službenicima agencije prilikom presuđivanja po žalbama.

Pitanje pravnih lijekova je najteže pitanje kada se radi o sistemima rješavanja žalbi. Uopćeno govoreći, tijela sa najvećom sposobnosti da nadoknade pogrešno postupanje obavještajne službe (sudovi) su najmanje sposobni da rješavaju žalbe vezane za specifične okolnosti koje se tiču obavještajnih službi, posebno zahtjeva tajnosti i zaštite klasificiranih informacija. Stručna tijela za nadzor često su bolje pozicionirana da se probijaju kroz tajnost, ali općenito nemaju ovlasti da učine više nego da daju preporuke. Države treba pažljivo da razmotre da li stručna nadzorna tijela koja imaju funkciju rješavanja žalbi

treba također da imaju kvazisudske ovlasti u pogledu pravnog lijeka, kao što je ovlast da dodjeljuju finansijsku nadoknadu za pogođene pojedince.

- Davanje tijelima za rješavanje žalbi samo ovlasti da daju preporuke nedovoljno je i ne predstavlja „učinkovit pravni lijek". Umjesto toga, ta tijela treba da dobiju kvazisudske ovlasti davanja pravnog lijeka, kao što je ovlast da se dodjeljuje finansijska naknada.

Konačno, države treba da izbjegnu isključivu ovisnost o modelu koji se zasniva na žalbi, kako bi se osigurala odgovornost obavještajne službe. Rješavanje žalbi svakako ima svoje mjesto u tom procesu. Međutim, iskustva nekih država koje se isključivo oslanjaju na tijela za rješavanje žalbi u vršenju te funkcije nisu pozitivna. U Kanadi, recimo, funkcije državne sigurnosti koje provodi federalna policija (RCMP) podložna su slabom mehanizmu odgovornosti koje se temelje na žalbama. Sudska istraga o sumnjivim praksama borbe protiv terorizma RCMP-a nakon 11. septembra preporučuje i pojačane ovlasti rješavanja žalbi i funkcioniranje sistema revizorske ocjene. Istraga je pokazala da „potreba za ocjenama na vlastitu inicijativu proizlazi iz činjenice da se većina aktivnosti RCMP-a provodi u tajnosti i ima malo, ako ima uopće, sudske kontrole, a ipak krije mogućnost da znatno utječe na prava i slobode pojedinaca. "[65]

Kratkovidost modela odgovornosti koji se temelje na žalbama rizikuje stvaranje jednog oblika „teatra" odgovornosti: postojanje tijela stvara privid kontrole, ali ono ne može učinkovito djelovati zbog tajnosti koja okružuje aktivnosti obavještajne službe. Ova tajnost može učiniti da osobe koje su predmet djelovanja obavještajnih službi nemaju saznanje, na primjer, o neovlaštenom kršenju njihovog prava na privatnost. Iz tog razloga, sistemi rješavanja žalbi uz koje ne idu drugi oblici nadzora, sposobni da razotkriju prekršaje, predstavljaju slab pristup demokratskog upravljanja obavještajnim agencijama.

- Isključiva ovisnost o modelu odgovornosti obavještajne službe koji se temelji na žalbi je neodgovarajuća. Takav pristup mora pratiti sistem nezavisne ocjene i/ili nadzora.

TABELA 1: SPISAK NAJBOLJIH PRAKSI RJEŠAVANJA ŽALBI	
Praksa	**Implikacije ako se ne poštuje praksa**
Da li je tijelo za rješavanje žalbi adekvatno osposobljeno za dato pitanje, te da li ima pravnu stručnost?	Ako nije, mogu se postaviti pitanja sposobnosti tijela za rješavanje žalbi da presuđuje u žalbama na učinkovit i vjerodostojan način.
Da li tijelo za rješavanje žalbi ima puni pristup tajnim informacijama obavještajne službe?	Ako nema, tijelo za rješavanje žalbi rizikuje da ne bude u stanju stvarno utvrditi meritum žalbi i ocijeniti aktivnosti službe.
Da li je tijelo za rješavanje žalbi nezavisno od vlade i obavještajne službe u pogledu procesa imenovanja, sigurnosti mandata, te upravljanja operacijama?	Ako nije, tijelo za rješavanje žalbi vjerovatno neće imati vjerodostojnost i možda, u stvari, neće moći donositi nezavisne odluke.
Da li tijelo za rješavanje žalbi dozvoljava i insajderske i javne žalbe?	Ako ne, insajderi mogu biti navedeni na to da se odluče da na prekršaj u službi upozore npr., medije, dok pripadnici javnosti imaju samo mogućnost da žalbe podnose općim sudovima ili drugim tijelima koja nisu dovoljno osposobljena da presuđuju u pitanjima državne sigurnosti.
Da li su insajderi zaštićeni od odmazde kada podnose žalbe u dobroj namjeri, bilo u vezi sa zakonom o zapošljavanju i/ili zakonom o službenoj tajni?	Ako ne, insajderi neće imati poticaja da učestvuju u procesu koji vode tijela za rješavanje žalbi ili će ih to odvratiti od toga da uopće otkrivaju prekršaje.
Da li zakoni omogućavaju bilo kom pripadniku javnosti da može podnijeti žalbu oko širokog spektra aktivnosti obavještajne službe?	Ako ne, legitimno pitanje o aktivnosti agencije može ostati neregistrirano.
Dok je opravdano pravo tijela za rješavanje žalbi da odbace nemeritorne žalbe, da li ona to pravo koriste pažljivo, ne odbacujući, na primjer, kao nemeritorne žalbe one koje mogu imati političke implikacije ili zbog ličnih osobina samog podnosioca žalbe?	Ako nije, legitimna pitanja u vezi sa aktivnostima agencije mogla bi previše lako biti odbačena.
Da li tijelo za rješavanje žalbi ima ovlast da donese odluke o kvazisudskim pravnim lijekovima, kao što je finansijska nadoknada?	Ako nema, odluke tijela za rješavanje žalbi može imati malo utjecaja na aktivnosti agencije, dok istovremeno može odvratiti podnosioce žalbe da uopće podnose žalbu.

Bilješke

1. Hans Born i Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway), str. 105.
2. Hans Born i Ian Leigh, *Democratic Accountability of Intelligence Services*, Policy Paper br. 19 (Geneva: DCAF, 2006) str. 17.
3. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* (henceforth Scheinin Report), United Nations Document A/HRC/14/46 (17. maj 2010), str. 10.
4. Scheinin Report, str. 10.
5. Scheinin Report, str.11 (gdje se navodi Čl. 2. Međunarodnog pakta o građanskim i političkim pravima)
6. *Klass v. FRG*, A 28 (1979), 2 EHHR 214 u stavu 64 (kojim se tumači Čl. 13. ECHR).
7. Scheinin Report, str. 11.
8. Canadian Security Intelligence Service Act (31. avgust 2004), R.S.C., Chapter C-23, Čl. 42. (dostupno http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
9. Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 28. i 30. (dostupno na http://www.comiteri.be/images/pdf/engels/w.toezicht - l.contrle - engelse versie.pdf).
10. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e) (2) (dostupno na http://codes.lstr.findlaw.com/uscode/50/15/I/403q).
11. Sjedinjene Države, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (d)(5)(G).
12. Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 18. (dostupno na http://www.legislation.govt.nz/act/public/1996/0047/latest/whole.html - dlm392526).
13. Sjedinjene Države, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3)(B).
14. Kanada, Security of Information Act (1985), R.S.C., Chapter O-5, Čl. 15. (dostupno na http://laws.justice.gc.ca/eng/acts/O-5/).
15. The Netherlands, Intelligence and Security Services Act (7. februar 2002), Čl. 83. (dopunjeno) (dostupno na http://www.ctivd.nl/?download=WIV 2002 Engels.pdf).
16. Irska, Garda Síochána Act 2005, br. 20 iz 2005, Čl. 67.
17. Canadian Security Intelligence Service Act (31. avgust 2004), R.S.C., Poglavlje C-23, Čl. 41. (dostupno na http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).
18. Sjedinjene Države, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3).
19. Kenija, National Security Intelligence Service Act (31. decembar 1998), Čl. 24. (dostupno na http://www.nsis.go.ke/act.pdf).
20. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 3. (1) (f) (dostupno na http://www.acts.co.za/intelligence_services_oversight_act_1994.htm).
21. Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 11.
22. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 8. (dostupno na http://www.comlaw.gov.au/Details/C2011C00349).
23. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010), str. 50 (gdje se razmatra Finska).
24. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010.) Stav 121 (gdje se kao mehanizam ulaganja žalbi za Benin navodi Ustavni sud; Stav 294 (gdje se kao glavno tijelo za žalbe za Ekvador navodi Ustavni sud); Stav 243 (isto, u vezi sa Kostarikom); Stav 307 (gdje se sudovi navode kao glavni mehanizmi za žalbe za osobu pogođenu praćenjem sigurnosne službe); Stav 353 (gdje se razmatra uloga sudova u vezi sa građanskim prekršajima koje počine obavještajne službe u Gruziji, te glavnog tužioca u vezi sa krivičnim djelima), Stav 482 (gdje sa razmatra sistem u Letoniji); Stavovi 556–557 (gdje sa razmatra sistem na Madagaskaru).
25. Holandija, Intelligence and Security Services Act, Čl. 83.
26. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental*

freedoms while countering terrorism: Addendum, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010), str. 49 (gdje se razmatra Finska); Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *International Models of Review of National Security Activities* (maj 2005), str. 14 (dostupno na http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/IntlModels_may26.pdf).

27. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010), Stavovi 67, 75, i 82 (gdje se razmatra Belgija); Stav 327 (gdje se razmatra Finska); Stav 374 (gdje se opisuju uloge grčke institucije ombudsmena); vidjeti i Kanada, Privacy Act (1985), R.S.C., Poglavlje P-21, Čl. 29. (dostupno na http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html).
28. Canadian Human Rights Act (1985), R.S.C., poglavlje H-6, Čl. 45–46. (dostupno na http://laws-lois.justice.gc.ca/eng/acts/H-6/page-15.html).
29. Za sudske predmete u kojima su zahtjevi vlade za čuvanjem tajne onemogućili (ili barem komplicirali) sposobnost podnosioca žalbe da dobije pravni lijek u građansko-pravnom postupku, vidjeti *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs,* [2009] EWHC 152 (Admin) (UK); *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs* [2009] EWHC 2549 (Admin) (UK); *Canada (Attorney General) v. Almalki*, 2011, FCA 199 (Kanada); *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. Cal. 2010) (Sjedinjene Države).
30. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, A *New Review Mechanism for the RCMP's National Security Activities* (2006), str. 492–3 (dostupno na http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006.pdf).
31. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010), Stav 380 (gdje se opisuje nadležnost odgovornog mađarskog ministra da prima žalbe u vezi sa mađarskim sigurnosnim agencijama); Stavovi 521–523 (gdje se razmatra sistem unutrašnje kontrole u Makedoniji); i Sjedinjene Države, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q.
32. Canadian Security Intelligence Service Act (31. avgust 2004), R.S.C., Poglavlje C-23, Čl. 35–37.
33. Kenija, National Security Intelligence Service Act (31. decembar 1998), Čl. 25.
34. Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 28. i 30.
35. Ujedinjeno Kraljevstvo, Investigatory Powers Tribunal web site (dostupno na http://www.ipt-uk.com/default.asp?ArtD=1).
36. Ujedinjeno Kraljevstvo, Investigatory Powers Tribunal web site (dostupno na http://www.ipt-uk.com/default.asp?sectionID=1).
37. Holandija, Intelligence and Security Services Act, Čl. 64. i 78.
38. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010) Stavovi 270 i 271 (gdje se opisuju funkcije hrvatskog Vijeća za civilni nadzor nad sigurnosno-obavještajnim agencijama); Stav 279 (gdje se opisuju funkcije Kiparskog nezavisnog tijela za istrage navoda i žalbi protiv policije); Stav 396 (gdje se opisuju funkcije Irske komisiije ombudsmena za Garda Síochána, stav 410 (gdje se opisuju funkcije japanske Prefekturalne komisiije za javnu sigurnost); Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 8 (dopunjeno).
39. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010) Stav 585; Norveška, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3. februar 1995), Čl. 3. (dostupno na http://www.eos-utvalget.no/filestore/EOSAct.pdf).
40. Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 34.
41. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 7(7)(cA).
42. Canadian Security Intelligence Service Act (31. avgust 2004), R.S.C., Poglavlje C-23, Čl. 41.
43. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1

(26 May 2010) Stav 270 (gdje se opisuje uloga hrvatskog parlamentarnog Odbora za unutarnju politiku i nacionalnu sigurnost); Stav 380 (gdje se opisuju funkcije mađarskog parlamentarnog Odbora za nacionalnu sigurnost); i stavovi 609–611 (gdje se opisuju rumunske zajedničke parlamentarne komisije, ali sugerira da će one istraživati žalbe samo uz blagoslov drugih parlamentarnih odbora); Larry Watts, "Control and Oversight of Security Intelligence in Romania," u Democratic Control of Intelligence Services, uredn. Hans Born I Marina Caparini (Aldershot, UK: Ashgate, 2007), str. 60 (gdje se razmatraju žalbe koje rješavaju rumunski parlamentarni odbori).

44. DCAF, Backgrounder: Parliamentary Oversight of Intelligence Services (2006) (gdje se zapaža da njemački parlamentarni "kontrolni panel" može rješavati žalbe građana); Njemačka, Control Panel Act (29. juli 2009), *Federal Law Gazette I*, str. 2346, Čl. 8.
45. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 3(1)(f).
46. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 10. (dopunjeno); Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 16.
47. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 11. (dopunjeno); Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 3(1)(f); Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 17.; Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 34.
48. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 19. (dopunjeno).
49. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 18. dopunjeno); Norveška, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3. februar 1995), Čl. 4. i 5; Njemačka, Control Panel Act (29. july 2009), *Federal Law Gazette I*, str. 2346, Čl. 5; Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 20. i 23; Kenya, National Security Intelligence Service Act (31. decembar 1998), Čl. 26; Belgija, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18. juli 1991), Čl. 48.
50. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 18. (dopunjeno).
51. Sjedinjene Države, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(2). Vidjeti i stavove (4) i (5).
52. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 5.
53. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 7.
54. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 7; Njemačka, Control Panel Act (29. juli 2009), *Federal Law Gazette I*, str. 2346, Čl. 10.
55. Južna Afrika, Intelligence Services Oversight Act (23. novembar 1994), Čl. 7; Vidjeti slična ograničenja u Norveškoj, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3. februar 1995), Čl. 9; Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 13.
56. Kanada, Security of Information Act (1985), R.S.C., Poglavlje O-5, shema.
57. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 17. (dopunjeno); Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 19; Kenija, National Security Intelligence Service Act (31. decembar 1998), Čl. 26.
58. Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 23 (dopunjeno).
59. Južna Afrika, Intelligence Services Oversight Act (23, novembar 1994), Čl. 5.
60. Kenija, National Security Intelligence Service Act (31. decembar 1998), Čl. 26.
61. Norveška, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), izdate na osnovu Čl. 1. Akta br. 7 od 3. februara 1995. u vezi sa Monitoringom obavještajnih službi, službi za praćenje i sigurnosnih službi, Čl. 8; Vidjeti i Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl.25.
62. Craig Forcese i Lorne Waldman, "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings" (studija naručena od Kanadskog centra za obavještajne i sigurnosne studije, uz finansijsku podršku Sudske administrative službe) (avgust 2007), str. 7–8.
63. Canadian Security Intelligence Service Act (31. avgust 2004), R.S.C., Poglavlje C-23, Čl. 52. (gdje se opisuju ovlasti SIRC-a); Holandija, Intelligence and Security Services Act, Čl. 84. (gdje se opisuju ovlasti Nacionalnog ombudsmena); United Nations Human Rights Council, *Report of the Special*

Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum, United Nations Document A/HRC/14/46/Add.1 (26. maj 2010) Stav 77 (gdje se opisuju ovlasti belgijskog povjerenika za zaštitu); i Stav 585 (gdje se opisuju ovlasti norveškog nadzornog odbora); Australija, Inspector-General of Intelligence and Security Act (17. oktobar 1986), Čl. 24. (dopunjeno); Norveška, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Norveška, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), izdate na osnovu Čl. 1. Akta br. 7 od 3. februara 1995. u vezi sa Monitoringom obavještajnih službi, službi za praćenje i sigurnosnih službi, Čl 8; Novi Zeland, Inspector-General of Intelligence and Security Act (1. juli 1996), Čl. 25; Kenija, National Security Intelligence Service Act (31. decembar 1998), Čl. 26.

64. Ujedinjeno Kraljevstvo, Investigatory Powers Tribunal web site, "Complaints process: What happens to my complaint?" (http://www.ipt-uk.com/sections.asp?sectionID=4&chapter=0&type=top); Ujedinjeno Kraljevstvo, Regulation of Investigatory Powers Act 2000, Poglavlje 23, Čl. 67.
65. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), str. 18.

O autorima

HANS BORN je viši naučni savetnik DCAF-a. Trenutno se bavi nadzorom nad obavještajnim službama kao i ulogom parlamenata i institucija ombudsmena u demokratskom upravljanju sigurnosnim sektorom. Specijalizirao se za Jugoistočnu Aziju (uključujući Kambodžu, Indoneziju, Filipine i Tajland). Bavio se istraživanjem politika u područjima ljudskih prava, odgovornosti i demokratskog upravljanja sigurnosnim sektorom za Ujedinjene nacije, Organizaciju za sigurnost i saradnju u Evropi, Vijeće Evrope i Evropski parlament. Jedan je od inicijatora Međuparlamentarnog foruma za demokratsko upravljanje sigurnosnim sektorom u Jugoistočnoj Aziji (www.ipf-ssg-sea.net) i Međunarodne konferencije za institucije ombudsmena za oružane snage (www.icoaf.org). Objavio je dosta radova na temu reforme i demokratskog upravljanja sigurnosnim sektorom. Najnovije publikacije uključuju *Governing the Bomb: Democratic accountability and civilian control of nuclear weapons* (Oxford University Press, 2011), *Accountability of International Intelligence Cooperation* (Routledge 2011) i *Parliamentary Oversight of the Security Sector: ECOWAS Parliament-DCAF Guide for West African Parliamentarians* (ECOWAS, 2011). Magisterij iz predmeta Javna uprava stekao je na UniverzitetuTwente, a doktorat iz društvenih nauka na Univerzitetu Tilburg (Holandija).

AIDAN WILLS je koordinator projekta u Istraživačkom odjelu DCAF-a, gdje se šest godina bavi demokratskim upravljanjem sigurnosnim i obavještajnim sektorom. Bio je glavni konsultant u izradi Zbirke dobrih praksi obavještajnih službi i njihovog nadzora koju su objavile Ujedinjene nacije. U skorije vrijeme je bio jedan od autora velike studije Evropskog parlamenta o *Parlamentarnom nadzoru nad sigurnosnim i obavještajnim službama u Evropskoj uniji, i jedan od urednika izdanja Međunarodna saradnja i odgovornost na polju obavještajnog rada*. Također je učestvovao u obuci tijela za nadzor nad obavještajnim i sigurnosnim službama diljem Evrope i Bliskog Istoka, te je dao doprinos u brojnim procesima izrade zakona. Aidan radi kao konsultant Vijeća Evrope, Evropskog parlamenta i Specijalnog izvjestioca UN-a (za ljudska prava i borbu protiv terorizma) u raznim aspektima upravljanja sigurnosnim sektorom i ljudskih prava. Trenutno radi na izradi zbirke *Globalni principi državne sigurnosti i prava na informaciju* u okviru projekta koji predvodi Open Society Foundation.

MONICA DEN BOER radi u Policijskoj akademiji Holandije, a članica je i Odbora za evropske integracije Savjetodavnog vijeća za međunarodne poslove. Doktorat je stekla 1990. godine na Evropskom univerzitetskom institutu, a radila je na Edinburškom univerzitetu,

Holandskom studijskom centru za kriminal i provedbu zakona, Evropskom institutu za javnu upravu, Univerzitetu u Tilburgu i Evropskom institutu za saradnju u provedbi zakona. Između marta 2004. i januara 2012. godine, predaje na predmetu Komparativna i javna uprava na Univerzitetu VU u Amsterdamu, u ime Policijske akademije Holandije. Godine 2009, bila je članica Holandskog iračkog istražnog odbora, a u periodu 2009-2010, učestvovala je u radu grupe Defence Future Survey Group. Objavila je brojne radove na temu unutarnje evropske sigurnosne saradnje, te drži predavanja, obuke i učestvuje u mentorstvu.

STUART FARSON je vanredni profesor političkih nauka na Univerzitetu Simon Fraser (Kanada). U periodu 1989-90, bio je direktor istraživanja u prvoj i jedinoj dosad parlamentarnoj ocjeni kanadskog Zakona o sigurnosno-obavještajnoj službi. Bio je vještak za Istražnu komisiju djelovanja kanadskih zvaničnika u vezi sa slučajem Maher Arar. U skorije vrijeme zajedno sa Regom Whitakerom napisao je knjigu "Accountability in and for National Security," IRPP Choices (2009). Također je bio jedan od urednika knjige Inquiry and National Security (2011) i PSI Priručnika o globalnoj sigurnosti i obavještajnom radu: Državni pristupi (2008), koje je objavila izdavačka kuća Praeger.

CRAIG FORCESE je zamjenik dekana i vanredni profesor na Pravnom fakultetu (Odsjek za običajno pravo), Univerziteta u Otawi. Predaje Javno međunarodno pravo, Pravo vezano za državnu sigurnost, Administrativno pravo i Javno pravo/legislativu. Najveći dio trenutnog istraživanja i autorskog rada odnosi se na državnu sigurnost, ljudska prava i demokratsku odgovornost. Trenutno je predsjednik Kanadskog vijeća za međunarodno pravo. Autor je, između ostalog, knjiga *National Security Law: Canadian Practice in International Perspective* (Irwin Law, 2008) i koautor *Human Rights and Anti-terrorism* (Irwin Law, 2008).

GABRIEL GEISLER MESEVAGE je doktorski kandidat na Institutu za međunarodne i razvojne studije, gdje također radi kao asistent. Radi i kao istraživač saradnik na istom Institutu, gdje proučava korupciju u privatnom sektoru. Od 2010-2011, Gabriel radi u Istraživačkom odjelu DCAF-a, gdje njegovo istraživanje usmjereno je na demokratsko upravljanje policijom i obavještajnim službama. Tokom rada za DCAF, Gabriel je dao doprinos u izradi priručnika o integritetu policije, urađenog u Odjelu za vanjski nadzor. Magistrirao je sa izvanrednim uspjehom Međunarodne odnose i socijalnu antropologiju na Univerzitetu St. Andrews (Ujedinjeno Kraljevstvo), te ima magisterij iz Međunarodnih studija koji je stekao na Institutu za međunarodne i razvojne studije.

LAUREN HUTTON od 2005 godine radi kao istraživač reforme sigurnosnog sektora i postkonfliktne transformacije Afrike, gde je učestvovala i u praktičnim aktivnostima reforme. Trenutno je savjetnica Danske grupe za demineriranje i Danskog vijeća za izbjeglice u Južnom Sudanu, pri čemu je fokus njenog djelovanja na osjetljivosti prema konfliktu i smanjenju oružanog nasilja. Lauren je prethodno radila za organizaciju Saferworld i za Institut za sigurnosne studije (ISS). Dok je bila angažirana na Institutu za sigurnosne studije, uradila je projekat demokratskog upravljanja obavještajnim službama u Africi. Kroz to je pružila input za proces ocjene obavještajnih službi, realiziran 2007. godine, te procese izrade zakona 2009. i 2010. godine u Južnoj Africi, te obučavala parlamentarce u južnoj i istočnoj Africi o nadzoru nad obavještajnim službama. Objavila je i knjigu o obavještajnom radu i demokratiji u Južnoj Africi, *To Spy or not to Spy*, te nekoliko članaka u časopisima. U tom je periodu povremeno objavljivala i radove o upravljanju obavještajnim službama. Magisterij Političkih nauka stekla je na Univerzitetu Western Cape (Južna Afrika).

IAN LEIGH je profesor prava na Univerzitetu u Durhamu i član Globalnog sigurnosnog instituta Durham. Objavio je, među ostalima, knjige *In From the Cold: National Security and Parliamentary Democracy* (Oxford University Press, 1994), sa Laurence Lustgarten, *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Potomac Books, 2005) sa Hansom Bornom i Lochom Johnsonom, i International Intelligence Cooperation and Accountability (Routledge, 2011), sa Hansom Bornom i Aidanom Willsom. Njegov izvještaj o politikama *Making Intelligence Accountable* (sa dr. Hansom Bornom, u izdanju Štamparske kuće Norveškog parlamenta, 2005. godine. preveden je na 14 jezika. Koautor je publikacije koju su objavili OSCE i DCAF *Handbook on Human Rights and Fundamental Freedoms of Armed Forces Personnel* (Varšava, 2008), te je radio kao konsultant OSCE-ovog Ureda za demokratske institucije i ljudska prava, Venecijanske komisije za demokratsku kontrolu nad sigurnosnim i obavještajnim agencijama u državama Vijeća Evrope kao i UNDP-a na polju reforme sigurnosnog sektora.

LAURIE NATHAN je vanredna profesorica i direktorica Centra za medijaciju na Unverizitetu Pretorija. Gostujući je profesor na Cranfield univerzitetu, gdje predaje na magistarskom studiju o reformi obavještajnih službi. Njena najnovija knjiga je *Community of Insecurity: SADC's Struggle for Peace and Security in Southern Africa*, Ashgate (2012). Bila je članica Ministarske komisije za ocjenu obavještajnih službi u Južnoj Africi (2006-8.) te je izradila White Paper on Defence (1996.) Južne Afrike. Članica je Savjetodavnog odbora Odjela naoružanja organizacije Human Rights Watch, Međunarodnog vijeća za rješavanje sukoba pri Carterovom centru, te stručne savjetodavne grupe za UNDP-ovu mrežu praksi demokratskog upravljanja. Članica je UN-ove liste kandidata za Medijaciju i liste stručnjaka za reformu sektora sigurnosti.

KENT ROACH je profesor prava na Univerzitetu u Torontu, gdje je šef Katedre Prichard Wilson za Pravo i Javnu politiku. Bio je član istraživačkih savjetodavnih odbora Komisije za istrage djelovanja kanadskih zvaničnika u vezi sa slučajem Maher Arar i direktor istraživanja Istražne komisije za istragu o bombama na letu Air India 182. Najnovija knjiga mu je *The 9/11 Effect: Comparative Counter-Terrorism*, u izdanju Cambridge 2011.

BERT VAN DELDEN pridružio se holandskom pravosuđu 1966. Bio je predsjednik Haškog okružnog suda u periodu 1990-2001. Godine, te je potom imenovan za prvog predsjednika Vijeća za pravosuđe. Nakon odlaska u penziju, imenovan je za člana holandskog Odbora za ocjenu obavještajnih i sigurnosnih službi (CTIVD). Od 2009, služi kao predsjednik tog Odbora.

THEODOR H. WINKLER je direktor Ženevskog centra za demokratsku kontrolu nad oružanim snagama (DCAF) od 2000. godine, kada ga je Švajcarsko savezno vijeće unaprijedilo u rang ambasadora i imenovalo za rukovodioca ovog novouspostavljenog centra. U Ministarstvu odbrane Švajcarske počeo je raditi krajem 1981. godine kao ekspert za međunarodnu sigurnost. Godine 1985. imenovan je za predstavnika načelnika za političko-vojna pitanja, a 1995. postaje rukovodilac novoformiranog Odjela za međunarodnu sigurnosnu politiku. Potom je unaprijeđen na mjesto zamjenika rukovodioca za sigurnosnu i odbrambenu politiku. Winkler je studirao političke nauke i međunarodnu sigurnost na Ženevskom univerzitetu, Harvardskom univerzitetu, kao i na Institutu za međunarodne studije u Ženevi. Doktorat iz političkih nauka sa tezom o proliferaciji nuklearnog oružja stekao je 1981. godine.

Nadzor nad obavještajnim službama

Priručnik

Ovaj priručnik je zbirka poglavlja čiji su autori vodeći eksperti za upravljanje obavještajnim radom iz cijelog svijeta. Priručnik nudi smjernice, koje su relevantne u pogledu politika, o uspostavi i konsolidaciji sistema nadzora nad obavještajnim službama, kao i za nadzor u ključnim oblastima rada obavještajnih službi kao što su prikupljanje informacija, korištenje ličnih podataka, razmjena informacija sa domaćim i stranim partnerima, i finansije. Smjernice su komparativne i temelje se na zakonskim i institucionalnim okvirima i praksama brojnih država.

Priručnik je usmjeren na parlamentarna i nezavisna nadzorna tijela i sadrži saznanja koja su relevantna za izvršnu vlast, sudstvo, medije, civilno društvo i same obavještajne službe. Ovaj priručnik vjerovatno će biti posebno zanimljiv članovima i osoblju nadzornih tijela; onima koji su uključeni u praćenje rada nadzornih tijela (npr., medije, organizacije civilnog društva i parlamentarce); subjekte vanjskog nadzora; izvršnu granu vlasti te obavještajne službe.

Ženevski centar za demokratsku kontrolu nad oružanim snagama (DCAF) je međunarodna fondacija čija je misija pomoći međunarodnoj zajednici u težnji za dobrim upravljanjem i reformom sigurnosnog sektora. Centar razvija i promovira norme i standarde, provodi specifična istraživanja na planu politika, identificira dobre prakse i preporuke radi promocije demokratskog upravljanja sigurnosnim sektorom, te pruža savjetodavnu podršku i programe praktične pomoći na licu mjesta u samim zemljama.

www.dcaf.ch