

Jelena Pejić

BEZBJEDNOSNO-OBAVJEŠTAJNI
SISTEMI U DRŽAVAMA ČLANICAMA
EVROPSKE UNIJE:
PRIMJERI HOLANDIJE I HRVATSKE



BEZBJEDNOSNO-OBAVJEŠTAJNI
SISTEMI U DRŽAVAMA ČLANICAMA
EVROPSKE UNIJE:
PRIMJERI HOLANDIJE I HRVATSKE

Beograd
jun 2016.

BEZBJEDNOSNO-OBAVJEŠTAJNI SISTEMI
U DRŽAVAMA ČLANICAMA EVROPSKE UNIJE:
PRIMJERI HOLANDIJE I HRVATSKE

Izdavač

Beogradski centar za bezbednosnu politiku
Đure Jakšića 6/5, Beograd
Telefon: 011 3287 226
E-mail: office@bezbednost.org
www.bezbednost.org

Autorka

Jelena Pejić

Urednici

Miroslav Hadžić
Predrag Petrović

Lektura i korektura

Tatjana Hadžić Jovović

Dizajn i prelom

Marko Marinković

Štampa

Unagraf

Tiraž

100

ISBN

978-86-6237-131-7

BEOGRAD, jun 2016.



Kingdom of the Netherlands

Objavljivanje ove publikacije podržala je Ambasada Kraljevine Holandije kroz projekat „LEGASI – Ka zakonodavnoj reformi bezbednosno-obaveštajnog sistema”. Stavovi izneti u ovoj publikaciji predstavljaju stavove autorke i ne odražavaju nužno stavove Kraljevine Holandije.

Sadržaj

OPŠTA SLIKA BEZBJEDNOSNO-OBAVJEŠTAJNIH SISTEMA HOLANDIJE I HRVATSKE	6
UPRAVLJANJE I KOORDINACIJA BEZBJEDNOSNO-OBAVJEŠTAJNOG SISTEMA	7
POLICIJSKA OVLAŠĆENJA SLUŽBI BEZBJEDNOSTI I NJIHOVO UČEŠĆE U KRIVIČNIM ISTRAGAMA	13
PRIMJENA POSEBNIH MJERA ZA TAJNI NADZOR KOMUNIKACIJA	14
Opšti uslovi.	14
Vrste tajnog nadzora nad komunikacijama.	15
Pristup zadržanim podacima o elektronskim komunikacijama	17
Položaj i uloga specijalizovanih tijela	18
UNUTRAŠNJA KONTROLA	19
SPOLJNA KONTROLA I NADZOR	20
Izvršni nadzor	21
Parlamentarni nadzor.	21
Specijalizovana nadzorna tijela	22
Nadzor koji vrše nezavisne državne institucije	25
Izvještavanje, obavještavanje i transparentnost	25
RELEVANTNI PRAVNI OKVIR.	27
Hrvatska	27
Holandija	27
LITERATURA.	29

OPŠTA SLIKA BEZBJEDNOSNO-OBAVJEŠTAJNIH SISTEMA HOLANDIJE I HRVATSKE

Kraljevina Holandija i Republika Hrvatska imaju po jednu civilnu i vojnu bezbjednosno-obavještajnu službu i njihov položaj regulisan je jedinstvenim obuhvatnim zakonom.

U **Holandiji** to su Opšta obavještajno-bezbjednosna služba (*Algemene Inlichtingen-en Veiligheidsdienst – AIVD*) i Vojna obavještajno-bezbjednosna služba (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*), predviđene *Zakonom o obavještajnim i bezbjednosnim službama* iz 2002. (ZOBS).¹ Opšta obavještajno-bezbjednosna služba (AIVD) u formi je generalnog direktorata u sastavu Ministarstva unutrašnjih poslova i kraljevskih odnosa, a nadležna je da vodi istrage o sumnjivim licima i organizacijama radi zaštite demokratskog poretka i vitalnih državnih interesa, da sprovodi bezbjednosne provjere i da štiti tajne podatke. U obavljanju ovih zadataka pomažu joj posebno određeni službenici regionalnih policija, Kraljevske holandske vojne policije i državne Poreske kancelarije Ministarstva finansija. Vojna obavještajno-bezbjednosna služba (MIVD) nalazi se u sastavu Ministarstva odbrane i prikuplja podatke, sprovodi istrage, vrši bezbjednosne provjere i čuva tajne podatke samo u vezi sa holandskim oružanim snagama. Saradnja između holandskih bezbjednosno-obavještajnih službi je sve intenzivnija, tako da su one ustanovile i zajednička tijela, poput Zajedničke sigint sajber jedinice (*Joint Sigint Cyber Unit – JSCU*)², a planiraju i zajedničko sjedište u budućnosti³. S obzirom na starost važećeg zakona, razvoj tehnologije i neke međunarodne skandale velikih razmjera, poput afere Snouden 2013. godine⁴, holandska Vlada predložila je novi Zakon o obavještajnim i bezbjednosnim službama⁵, tako da će sistem opisan u ovoj analizi vjerovatno uskoro pretrpjeti izmjene.

Hrvatska ima Sigurnosno-obavještajnu agenciju (SOA) i Vojnu sigurnosno-obavještajnu agenciju (VSOA) u okviru Ministarstva obrane. Njihovi zadaci i status uređeni su *Zakonom o sigur-*

1 Staatsblad van het Koninkrijk der Nederlanden 148 2002, 574 2006.

2 Sigint je skraćenica od eng. „signals intelligence” i podrazumijeva prikupljanje podataka presretanjem signala, uključujući u to i one signale (analogne i digitalne) od kojih se sastoji elektronska komunikacija. Sajber se odnosi na infiltriranje ili zaštitu računarskih i informacionih sistema. Zajednička sigint sajber jedinica (JSCU) formirana je kao zajedničko tijelo sporazumom između AIVD-a i MIVD-a o Zajedničkoj sigint sajber jedinici od 3. jula 2014. godine. <<https://zoek.officielebekendmakingen.nl/blg-359723.pdf>> 23. 3. 2016.

3 AIVD Annual Report 2014: 40. <<https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2015/05/13/annual-report-2014-not-only-returnees-but-also-%E2%80%9Cstay-at-homes%E2%80%9D-pose-a-threat/annual-report-aivd-2014.pdf>> 23. 12. 2015. Saradnja između AIVD-a i MIVD-a predviđena je, sa znatno manjim zamahom, u članu 58 ZOBS-a.

4 Počev od juna 2013. godine mediji su, na osnovu podataka koje im je dostavio uzbunjivač Edvard Snouden, otkrili masovno prisluškivanje telefonskih razgovora koje su vršili američka Državna bezbjednosna agencija (NSA) i njeni partneri u Evropi. Meta su bili, kako obični građani, tako i diplomate. Skandal je pokrenuo globalnu debatu o masovnom nadzoru i kontroli bezbjednosnih službi. Za kratak pregled o temi vidjeti, na primjer, <<http://www.dw.com/sr/godinu-dana-afere-snouden/a-17681790>> 13. 4. 2016.

5 Verzija Nacrta iz juna 2015. dostupna je na: <<https://www.internetconsultatie.nl/wiv/document/1715>> 15. 2. 2016.

nosno-obavještajnom sustavu iz 2006. godine (ZSOS).⁶ Sigurnosno-obavještajna agencija štiti nacionalnu bezbjednost prikupljanjem i analizom podataka u zemlji i inostranstvu, te vrši bezbjednosne provjere, dok VSOA štiti Ministarstvo obrane i hrvatske Oružane snage. Pored ove dvije službe⁷, ZSOS predviđa i tri upravljačko-koordinatorna tijela i dva posebizovana tijela u hrvatskom bezbjednosno-obavještajnom sistemu. U prvu grupu spadaju Vijeće za nacionalnu sigurnost, koje usmjerava rad službi, Savjet za koordinaciju sigurnosno-obavještajnih agencija, koji operativno usklađuje njihov rad, i Ured Vijeća za nacionalnu sigurnost (UVNS), koji obavlja stručne poslove za Vijeće i Savjet. U drugoj grupi nalaze se Operativno-tehnički centar za nadzor telekomunikacija (OTC) i Zavod za sigurnost informacijskih sustava (ZSIS).

UPRAVLJANJE I KOORDINACIJA BEZBJEDNOSNO-OBAVJEŠTAJNOG SISTEMA

U Holandiji je upravljačko-koordinatorna uloga zakonski prepuštena nadležnim ministrima, kojima pomaže koordinator obavještajno-bezbjednosnih službi. Na podzakonskom nivou su, međutim, osnovani i Savjet za obavještajno-bezbjednosne službe, kao pododbor Vlade, i njemu podređen Zajednički obavještajni komitet. U Hrvatskoj Vijeće za nacionalnu sigurnost upravlja, a Savjet za koordinaciju sigurnosno-obavještajnih agencija koordinira radom službi. U izvršenju ovih zadataka pomaže im Ured Vijeća za nacionalnu sigurnost, koji ima jaka ovlaštenja. Članstvo u hrvatskom Vijeću i Savjetu šire je nego u ekvivalentnim holandskim tijelima, a uključuje i čelnike službi i UVNS-a. U Holandiji je članstvo podijeljeno, tako da u Savjetu sjede ministri, a u Komitetu koordinator i direktori službi, koji imaju pravo da prisustvuju i sastancima Savjeta. U hrvatskom Vijeću ovo pravo dato je predsjedniku parlamenta. U obje zemlje najviše upravljačko-koordinatorna tijela okupljaju premijere, te ministre unutrašnjih i spoljnih poslova, odbrane i pravde.

Kada je riječ o regulisanju upravljanja i koordinacije službi bezbjednosti, holandski i hrvatski zakon znatno se razlikuju. Odredbe holandskog ZOBS-a sasvim su šture⁸, prepuštajući upravljačku i koordinacionu ulogu nadležnim ministrima. Tijela koja im u tome pomažu sasvim su izostavljena. Čak i funkcijama koje se spominju, poput koodinatora i direktora službi, nije posvećena veća pažnja – ne uređuju se posebno njihova ovlaštenja niti propisuju bilo kakvi uslovi za njihov (re)

6 Narodne novine 79/06, 105/06.

7 Termin „službe” u nastavku teksta uvijek označava bezbjednosno-obavještajne službe, i to AIVD i MIVD u Holandiji, odnosno SOA i VSOA u Hrvatskoj.

8 Članovi 2–5 ZOBS-a.

izbor ili razrješenje. U hrvatskom ZSOS-u su, s druge strane, odredbe o ovom predmetu brojne i detaljne.

Bezbjednosno-obavještajne službe u **Holandiji** izričito su podređene nadležnim ministrima, koji usmjeravaju njihov rad, donose podzakonska akta o njihovoj organizaciji, te odobravaju primjenu posebnih mjera za tajno prikupljanje podataka.⁹ Za AIVD to je ministar unutrašnjih poslova i kraljevskih odnosa (MUPKO), a za MIVD ministar odbrane. Zakon ne predviđa institucionalizovan savjet, već redovne konsultacije ovih ministara o usmjeravanju rada službi i njihovoj koordinaciji, a po potrebi se mogu zvati i drugi ministri da učestvuju. Njima pomaže koordinator bezbjednosno-obavještajnih službi, koji odgovara premijeru, odnosno ministru opštih poslova.¹⁰ Zakon predviđa njegovo imenovanje kraljevskim ukazom na zajednički prijedlog nadležnih ministara, sa zadatkom da priprema međuresorne konsultacije i usklađuje rad AIVD-a i MIVD-a. Zakon spominje šefove službi¹¹, ali o njihovom izboru i mandatu ne kaže ništa, dok su im ovlaštenja rasuta po raznim članovima¹². Šefovi službi dužni su da sarađuju sa koordinatorom, prevashodno dostavljanjem svih neophodnih podataka.

Koordinaciona tijela, međutim, postoje, iako nisu predviđena ni postojećim Zakonom ni Nacrtom novog zakona. Neposredno nakon terorističkog napada u Madridu 2004. godine osnovan je Savjet za nacionalnu bezbjednost, a danas je to Savjet za obavještajno-bezbjednosne službe (*Raad voor de Inlichtingen-en Veiligheidsdiensten – RIV*). Savjet za obavještajno-bezbjednosne službe jeste pododbor holandske Vlade i čine ga predsjednik Vlade i njegov zamjenik, te ministri odbrane, unutrašnjih i kraljevskih poslova, spoljnih poslova i ministar bezbjednosti i pravde, a sastancima prisustvuju i Nacionalni koordinator za borbu protiv terorizma i bezbjednost¹³, kao i oba šefa službi. U okviru ovog pododbora razmatraju se analize službi o bezbjednosnoj situaciji, njihovi tromjesečni i godišnji izvještaji, kao i godišnji planovi rada. Tijelo koje priprema sastanke RIV-a jeste Holandski zajednički obavještajni komitet (*Comité Verenigde Inlichtingendiensten Nederland – CVIN*), na čijem je čelu koordinator službi, a članovi su šefovi obje službe, Nacionalni koordinator za borbu protiv terorizma i bezbjednost i predstavnik Ministarstva spoljnih poslova.

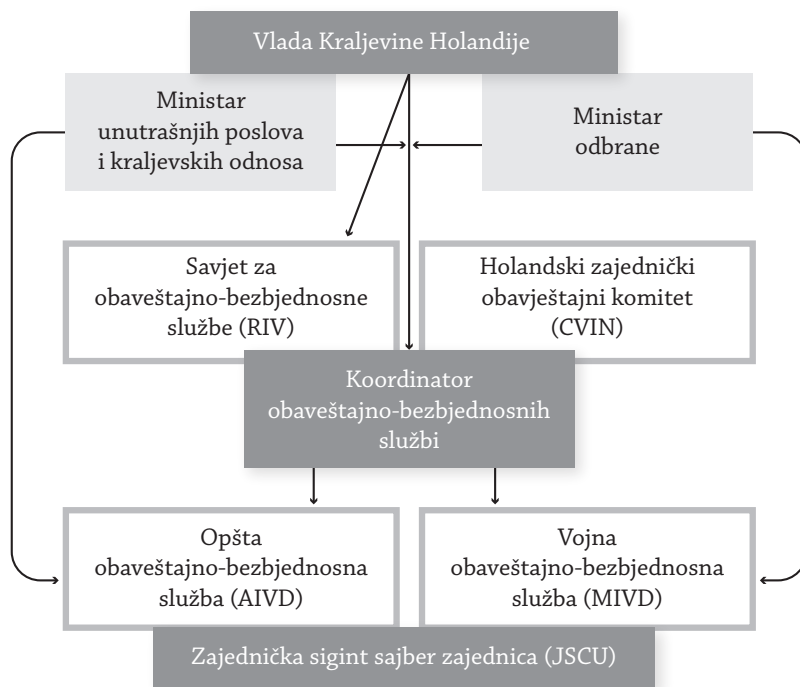
9 Članovi 2, 3, 11 i 19–29 ZOBS-a.

10 Koordinator je ujedno i šef kabineta premijera i generalni sekretar Ministarstva opštih poslova.

11 Za AIVD to je generalni direktor, za MIVD to je direktor.

12 Oni, na primjer, predlažu i nalažu pojedine posebne mjere tajnog prikupljanja podataka, staraju se o povjerljivosti i kvalitetu tih podataka i njihovih izvora, te odgovaraju za njihovu bezbjednost. Vidjeti članove 15–16 i 19–29 ZOBS.

13 Nacionalni koordinator za borbu protiv terorizma i bezbjednost djeluje u okviru Ministarstva bezbjednosti i pravde i ne treba ga miješati sa pomenutim koordinatorom bezbjednosno-obavještajnih službi. Zadatak Nacionalnog koordinatora je da djeluje preventivno na očuvanju društvene stabilnosti i umanjuju društvenih poremećaja. Za ocjenu stepena terorističke prijetnje u Holandiji koristi i podatke koje mu dostavlja AIVD. Nije ovlašten za primjenu posebnih mjera. Osnovan je Uredbom ministra bezbjednosti i pravde i MUPKO 2005. godine. Vidjeti: Regeling van de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties van 29 juni 2005, nr. DDS5357209, houdende instelling van de Nationaal Coördinator Terrorismedbestrijding <<http://wetten.overheid.nl/BWBR0018506/2010-10-10>> 20. 4. 2016.



Šema 1: Holandski bezbjednosno-obavještajni sistem¹⁴

Zakon u članu 60 predviđa da zadatke AIVD-a mogu obavljati i pripadnici regionalnih policija, komandant Kraljevske holandske vojne policije i generalni direktor državne Poreske kancelarije Ministarstva finansija. Šefovi regionalnih policija, ministar odbrane i ministar finansija uz saglasnost ministra unutrašnjih poslova i kraljevskih odnosa postavljaju niže službenike za obavljanje konkretnih zadataka i nadzor nad njihovim izvršenjem. Ovi službenici djeluju po uputstvima generalnog direktora AIVD-a, a odgovornost za njihovo djelovanje snosi MUPKO.

Zajednička sigint sajber jedinica nije predviđena Zakonom, već je ustanovljena naknadno sporazumom između nadležnih ministara. Ona za obje službe obavlja tajni nadzor nad elektronskim komunikacijama, kao i zaštitu i infiltraciju informacionih sistema. Prema sporazumu, u ovoj jedinici rade službenici AIVD-a i MIVD-a, na čelu sa izvršnim direktorom JSCU. Izvršni direktor zajedno sa šefovima službi čini Upravni odbor JSCU, koji se bavi menadžmentom i strateškim upravljanjem. U Upravnom savjetu, koji okuplja generalne sekretare Ministarstva unutrašnjih poslova i kraljevskih odnosa, Ministarstva odbrane i Ministarstva opštih poslova (ujedno koordinator službi), raspravlja se o političko-upravnim aspektima rada JSCU.¹⁵

¹⁴ Zakonom predviđena tijela su u plavim poljima.

¹⁵ Član 2 Sporazuma o JSCU iz 2014.

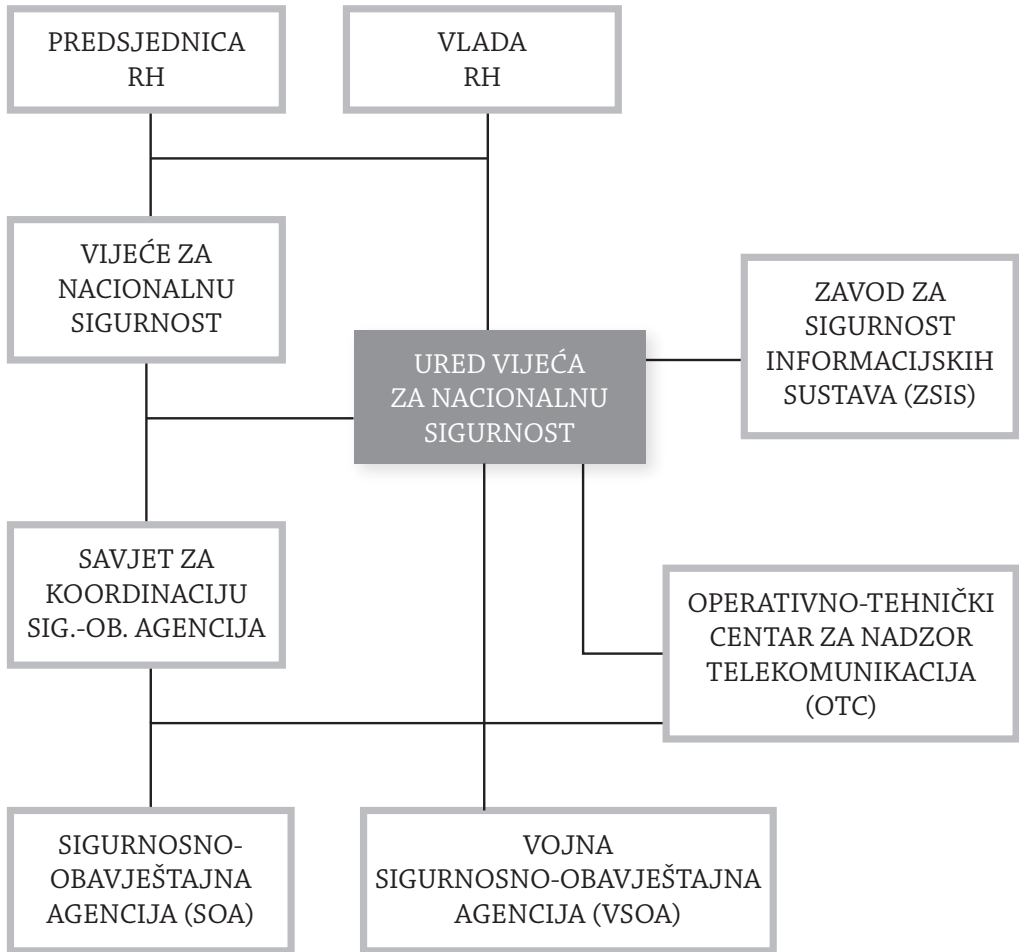
U **Hrvatskoj** Vijeće za nacionalnu sigurnost, Savjet za koordinaciju sigurnosno-obavještajnih agencija i Ured Vijeća za nacionalnu sigurnost predstavljaju sponu između službi, s jedne strane, i predsjednika i premijera, s druge strane. Vijeće usmjerava rad bezbjednosno-obavještajnih službi, Savjet vrši operativno usklađivanje, dok Ured obavlja stručne i administrativne poslove za oba tijela.

Vijeće za nacionalnu sigurnost čine predsjednik Republike i predsjednik Vlade, ministri unutrašnjih i spoljnih poslova, odbrane i pravosuđa, te savjetnik predsjednika Republike za državnu bezbjednost, načelnik Glavnog stožera Oružanih snaga RH, direktori obje agencije i načelnik UVNS-a. U radu Vijeća učestvuje, ali nije član, predsjednik Hrvatskog sabora. Predsjednik Republike i premijer zajednički sazivaju sjednice, utvrđuju dnevni red, te supotpisuju odluke Vijeća, dok predsjednik predsjedava sjednicama.¹⁶

Savjet za koordinaciju sigurnosno-obavještajnih agencija čine ministar unutrašnjih poslova u svojstvu predsjednika Savjeta, te savjetnik predsjednika Republike za državnu bezbjednost, u svojstvu zamjenika, kao i direktori bezbjednosno-obavještajnih agencija i načelnik UVNS-a. Predsjednik Savjeta i njegov zamjenik sazivaju sjednice najmanje jednom mjesečno, utvrđuju dnevni red i supotpisuju odluke Savjeta. U radu ovog tijela po pozivu mogu učestvovati i druga lica, od kojih su neka posebno naznačena u Zakonu.¹⁷

¹⁶ Članovi 3–4 ZSOS-a.

¹⁷ To su: javni tužilac (Glavni državni odvjetnik), direktor USKOK-a (Ured za suzbijanje korupcije i organizovanog kriminala, u sklopu Javnog tužilaštva), direktor Policije, direktor Carine, direktor Financijske policije, direktor Ureda za sprječavanje pranja novca, predstavnik Ministarstva vanjskih poslova zadužen za poslove bezbjednosti, direktor Uprave za zaštitu i spašavanje te čelnici drugih odgovarajućih inspekcijskih i nadzornih tijela. Vidjeti član 5 ZSOS-a.



Šema 2: Bezbjednosno-obavještajni sistem Republike Hrvatske¹⁸

Ured Vijeća za nacionalnu sigurnost (UVNS) pomaže Vijeću i Savjetu u obavljanju njihovih funkcija. Ured prima izvještaje o radu službi, analizira ih i ocjenjuje bezbjednosnu situaciju u sopstvenim periodičnim izvještajima. Posredstvom ovog tijela omogućava se nadzor izvršne vlasti nad radom službi, kao i Operativno-tehničkog centra. Na čelu UVNS-a nalazi se načelnik (predstojnik), koga imenuju i razrješuju zajedno predsjednik i premijer, na jednom obnovljiv mandat od četiri godine.¹⁹

18 Preuzeto sa zvaničnog sajta UVNS-a. <<http://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh>.>
12.4.2016.

19 Članovi 6–12 ZSOS-a.

Na čelu bezbjednosno-obavještajnih službi su direktori (ravnatelji) sa zamjenicima, a sve ih imenuju i razrješuju zajedno predsjednik i premijer. Hrvatski sabor učestvuje u izboru tako što njegov nadležni odbor daje mišljenje o prijedlogu kandidata, može kandidata pozvati na razgovor, a ima pravo i da, pored predsjednika i premijera, pokrene postupak za razrješenje direktora, i to iz jednog od sedam pobrojanih razloga.²⁰ Direktori imaju četvorogodišnji mandat, koji se može obnavljati neograničen broj puta.²¹

U hrvatskom bezbjednosno-obavještajnom sistemu prepoznajemo i dva specijalizovana tijela, koja imaju funkcije slične onima objedinjenim u holandskoj JSCU. Operativno-tehnički centar (OTC) obavlja tajni nadzor nad elektronskim komunikacijama za obje službe i druge nadležne organe, a Zavod za sigurnost informacionih sustava (ZSIS) obezbjeđuje informacione sisteme ne samo službi već i ostalih državnih tijela. Na čelu oba tijela nalaze se direktori koje imenuje Vlada, na prijedlog Savjeta za koordinaciju rada bezbjednosno-obavještajnih službi, na četvorogodišnji mandat, koji se može neograničeno obnavljati. Direktori izvještaje o radu dostavljaju jedino UVNS-u.²²

20 To su: „ako to sami zatraže; ako trajno izgube sposobnost obavljati svoju dužnost; ako ne provode odluke predsjednika Republike i Vlade kojima se usmjerava rad sigurnosno-obavještajnih agencija ili ne provode njihove mjere u svezi s nadzorom rada; zbog povrede Ustava, zakona ili drugih propisa; zlouporabe položaja ili prekoračenja ovlasti; zbog povrede tajnosti klasificiranih podataka te osude za kazneno djelo koje ih čine nedostojnima obavljanja dužnosti.” (član 66(4) ZSOS-a)

21 U Hrvatskom saboru je 2013. odbijen prijedlog za unošenje zakonskog ograničenja direktorskog mandata na dva puta uzastopno, uz obrazloženje da se pitanje još nije javilo u praksi, te potreba za preduzimanjem postupka izmjene zakona još nije opravdana. Vidjeti: *Izvešće Odbora za unutarnju politiku i nacionalnu sigurnost o Prijedlogu zakona o dopuni Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske*, P. Z. 254. <<http://www.sabor.hr/Default.aspx?art=54101>> 11. 4. 2016.

22 Članovi 13–22 ZSOS-a.

POLICIJSKA OVLAŠĆENJA SLUŽBI BEZBJEDNOSTI I NJIHOVO UČEŠĆE U KRIVIČNIM ISTRAGAMA

Hrvatske i holandske bezbjednosno-obavještajne službe nemaju policijska ovlašćenja, odnosno ne učestvuju u krivičnim istragama. Razdvajanje ovlašćenja je u Holandiji izričito, a u Hrvatskoj prećutno.

U članu 9 holandskog ZOBS-a ovo je izričito naglašeno. Pošto određeni službenici regionalnih policija prikupljaju podatke za AIVD, u članu 14 se ponavlja da ta aktivnost mora da bude strogo odvojena od prikupljanja podataka u druge svrhe. O tome detaljnija uputstva izdaje generalni direktor AIVD-a. U hrvatskom ZSOS-u policijska ovlašćenja se ne spominju. Zakon o kaznenom postupku (ZKP)²³ takođe izostavlja bezbjednosno-obavještajne službe kada nabraja organe nadležne za sprovođenje istražnih i posebnih dokaznih radnji.²⁴

To ne znači da ne postoji saradnja između službi i organa koji vrše krivičnu istragu. U Hrvatskoj su službe dužne obavijestiti Državno odvjetništvo ako tokom vršenja svojih zadataka otkriju krivično djelo koje se goni po službenoj dužnosti. Predviđeno je i zaključenje sporazuma o saradnji između SOA i Ministarstva unutarnjih poslova.²⁵ U Holandiji su zakonom predviđene mogućnosti za saradnju veće. Obavještavanje teče u oba smjera. Službe dostavljaju Javnom tužilaštvu podatke ne samo o otkrivenom krivičnom djelu već sve podatke za koje smatraju da su bitni za vođenje krivične istrage. Jedini uslov je da prethodno dobiju odobrenje nadležnog ministra.²⁶ Takođe, Javno tužilaštvo i pripadnici policije obavijestit će službe o podacima koji mogu njima biti zanimljivi, a mogu sazvati i uzajamne konsultacije.²⁷

23 Narodne novine 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14.

24 Istražne radnje sprovode javni tužilac, istražilac i policija (član 242(4) ZKP-a), a posebne dokazne radnje (tj. posebne mjere) sprovodi policija (član 337 ZKP-a).

25 Član 50 ZSOS-a.

26 Član 38 ZOBS-a.

27 Član 61 ZOBS-a.

PRIMJENA POSEBNIH MJERA ZA TAJNI NADZOR KOMUNIKACIJA

Hrvatske i holandske bezbjednosno-obavještajne službe ovlaštene su da prikriveno prikupljaju podatke, u šta je uključen i tajni nadzor nad komunikacijama. U obje zemlje sudsko odobrenje za primjenu ove posebne mjere neophodno je samo za presretanje poštanske prepiske, a u Hrvatskoj i za presretanje elektronskih komunikacija. Za pristup zadržanim podacima o elektronskoj komunikaciji bez uvida u njen sadržaj, međutim, dovoljan je nalog direktora službe. Tajni nadzor nad elektronskim komunikacijama za službe u obje zemlje sprovode specijalizovana tijela.

Opšti uslovi

Tajni nadzor nad elektronskim komunikacijama jedna je od posebnih mjera kojima službe, u okviru svojih nadležnosti, prikriveno prikupljaju podatke o licima. Kako se ovom mjerom zadire u jedno od osnovnih i ustavno zajemčenih građanskih prava – nepovredivost prepiske, odnosno sloboda i tajnost svih oblika komunikacije²⁸ – neophodno je pravno urediti i ograničiti njenu primjenu. Holandski i hrvatski ustavi dozvoljavaju jedino ono zadiranje u privatnu komunikaciju koje je predviđeno zakonom. Holandski Ustav dodatno insistira na tome da za primjenu ove mjere mora postojati prethodno odobrenje zakonski određenog tijela – za pismenu prepisku to je sud, dok za elektronsku („telefon i telegram”) nije specificirano. I u Hrvatskoj se sudsko odobrenje zahtijeva samo za primjenu intruzivnijih mjera, ali tek na zakonskom nivou. Hrvatski Ustav ne spominje ovaj uslov, ali propisuje dvije jedino legitimne svrhe ograničenja nepovredivosti komunikacije: zaštita nacionalne bezbjednosti i vođenje krivičnog postupka. To je ponovljeno i u relevantnim zakonima²⁹, dok u holandskom Ustavu i ZOBS-u ovakve napomene nema³⁰. Takođe, zakonske odredbe obje zemlje postavljaju dodatne preduslove za preduzimanje posebnih mjera – one se mogu primijeniti samo kao krajnje sredstvo, onda kada je podatke nemoguće prikupiti ili ih je veoma otežano prikupiti na drugi način, dok se prednost uvijek daje manje intruzivnoj mjeri.³¹

28 Član 13 holandskog Ustava, član 36 hrvatskog Ustava.

29 Član 33 ZSOS-a, član 109 Zakona o elektroničkim komunikacijama.

30 Iste dvije svrhe, međutim, navode se u članu 11.13 holandskog Zakona o telekomunikacijama iz 1998. godine.

31 Na primjer, smatra se da uvid u podatke o komunikaciji manje zadire u privatnu sferu pojedinca nego uvid u sadržaj njegove komunikacije. Članovi 31–32 holandskog ZOBS-a, član 33 hrvatskog ZSOS-a.

Kao vojne bezbjednosno-obavještajne službe, VSOA i MIVD imaju ograničen domen djelovanja – u Hrvatskoj u pogledu lica prema kojima mogu preduzimati posebne mjere (samo prema zaposlenicima, odnosno pripadnicima Ministarstva obrane i Oružanih snaga), a u Holandiji je ograničenje prostorno-funkcionalno (samo u MO ili u vezi sa prostorijama koje koristi Ministarstvo odbrane).³² Međutim, MIVD može da izađe izvan ovog ograničenja uz saglasnost MUPKO ili direktora službe, zavisno od posebne mjere koja se primjenjuje.

Vrste tajnog nadzora nad komunikacijama

Holandski ZOBS detaljno uređuje oblast tajnog nadzora nad različitim vrstama komunikacija, tako što svakoj posvećuje jedan zaseban član.³³ Kao opšte pravilo važi da primjenu posebnih mjera odobrava nadležni ministar, ili šef službe uz obavještenje nadležnog ministra, na maksimalno trajanje od tri mjeseca, koje se po zahtjevu može više puta obnovljati.³⁴ Ukupno trajanje primjene mjere, dakle, zakonski nije ograničeno, niti postoji prethodna sudska kontrola. Takođe, od opšteg pravila predviđeno je i niz izuzetaka, koji važe za pojedine mjere.

Zakon pravi jasnu razliku između kablovskih i nekablovskih telekomunikacija, dozvoljavajući ciljani nadzor³⁵ za obje, a opšti samo za potonje. Od 2002, kad je ZOBS usvojen, tehnološki razvoj doveo je do toga da su skoro sve elektronske komunikacije kablovske – telefonija, internet, e-pošta, društvene mreže, dok u manju grupu spadaju nekablovske komunikacije putem satelita i radio-talasa. U Holandiji je za presretanje kablovskih komunikacija neophodno da nadležni ministar odobri zahtjev šefa službe sa sljedećim sadržajem: predložena mjera, podaci o pogođenom licu i valjan razlog.³⁶ S druge strane, za primanje i snimanje nekablovskih komunikacija nije potrebno nikakvo odobrenje ukoliko je ono: a) neciljano ili b) ciljano za međunarodne komunikacije koje su vezane za vojne poruke (važi za MIVD).³⁷ Obaveza da se pribavi odobrenje nastaje samo ukoliko službe otkriju i zabilježe identitet lica ili organizacije koji su izvor prekogranične komunikacije, jer tada nadzor prestaje da bude samo opšti. Takođe, odobrenje je neophodno i radi odabira podataka o određenom licu ili temi iz mase primljenih komunikacija. Ako se odabir vrši na osnovu podataka o identitetu ili broju objekta ili nekoj drugoj tehničkoj karakteristik, odobrenje daje ministar unutrašnjih poslova i kraljevskih odnosa³⁸ na

32 Član 26 ZSOS-a, članovi 20, 22–25 i 28 ZOBS-a.

33 Članovi 25–29 ZOBS-a. Danas su ove odredbe uglavnom zastarjele i prve su na udaru predloženih zakonskih izmjena.

34 Član 19 ZOBS-a.

35 Nadzor koji je usmjeren na određen broj ili lice.

36 Član 25 ZOBS-a.

37 Član 26 ZOBS-a.

38 Saglasnost ovog ministra je neophodna i ako zahtjev dolazi od MIVD-a.

zahtjev direktora službe za period od najviše tri mjeseca, a potom po zahtjevu i neograničeno obnovljivo. Ako se odabir pak vrši na osnovu definisanih ključnih riječi, odobrenje istog ministra važi za obnovljiv period od maksimalno godinu dana. Period primjene je duži jer se ovakva selekcija smatra manje intruzivnom pošto nije usmjerena na konkretno lice, već na temu. Tema za koju su definisane ključne riječi mora biti detaljno opisana u zahtjevu šefa službe, kao i razlog za primjenu mjere. O sadržaju ovog zahtjeva i dobijenom ministarskom odobrenju mora se povjerljivo obavijestiti parlament i Nadzorna komisija za obavještajne i bezbjednosne službe (CTIVD), koja predstavlja stručno tijelo. Podaci koji ostanu izvan odabira mogu se čuvati najviše godinu dana.

Hrvatski zakonodavac je, s druge strane, mjere tajnog nadzora nad komunikacijama pobrojao na jednom mjestu – u članu 33(3) ZSOS-a. Od tajnog nadzora nad poštanskim i drugim pošiljkama razlikuje tajni nadzor telekomunikacija, koji obuhvata četiri mjere: (1) nadzor nad njihovim sadržajem; (2) nadzor nad podacima o telekomunikacijskom saobraćaju; (3) nadzor nad lokacijom korisnika i (4) nadzor nad međunarodnim telekomunikacijskim vezama. Među njima, stroži režim važi za mjere koje se smatraju intruzivnim – nadzor nad sadržajem telekomunikacija i nad poštanskom prepiskom. Prijedlog za njihovu primjenu podnose direktori službi, a nalog za sprovođenje daje jedan od sudija Vrhovnog suda Republike Hrvatske, kojeg odredi predsjednik Suda. Izuzetno, u hitnim slučajevima sprovođenje može započeti odmah na osnovu naloga direktora službe, uz trenutno obavještenje nadležnog sudije, koji u roku od 24 sata izdaje ili odbija da izda nalog. U slučaju da izdavanje prethodnog ili naknadnog naloga bude odbijeno, primjena mjere se obustavlja, prikupljeni podaci se uništavaju, dok je nadležni sudija dužan da o razlozima odbijanja obavijesti UVNS. I prijedlog i nalog imaju status tajnih podataka, moraju biti u pisanoj formi i sadržati naznaku mjere, naznaku objekta, obrazloženje i rok trajanja mjere.³⁹ Ako se više mjera predlaže odjednom, za svaku je potrebno posebno navesti propisane podatke. Ovakvim insistiranjem na preciznosti smanjuju se mogućnosti zloupotrebe.

Dok Zakon nekoliko puta naglašava da primjena posebnih mjera može da bude samo privremena, izričito i precizno ograničenje od četiri mjeseca predviđeno je samo za mjere u strožem režimu. Produženje primjene je moguće, ali podrazumijeva nešto složeniji postupak. Naime, u tom slučaju odlučuje vijeće od troje nadležnih sudija Vrhovnog suda, koje može da traži dodatna obrazloženja od direktora službi, kao i stručno mišljenje od UVNS-a.⁴⁰ Ostale tri mjere tajnog nadzora nad komunikacijama odobravaju direktori službi pisanim i obrazloženim nalo-

39 Član 36 ZSOS-a.

40 Član 37 ZSOS-a.

gom u okviru djelokruga rada službi. O izdatim nalogima, čiji sadržaj nije preciziran, dužni su mjesečno izvještavati UVNS.⁴¹

Pristup zadržanim podacima o elektronskim komunikacijama

Tajnim nadzorom nad elektronskim komunikacijama bave se i hrvatski *Zakon o elektroničkim komunikacijama* (ZEK)⁴², praćen *Uredbom o obvezama iz područja nacionalne sigurnosti za pravne i fizičke osobe u telekomunikacijama* (UEK)⁴³, te holandski *Zakon o telekomunikacijama* (ZT)⁴⁴. Ovim zakonima obavezuju se svi operateri komunikacijskih mreža ili usluga u obje zemlje da vode evidenciju o svojim krajnjim korisnicima, tako da se oni mogu identifikovati.⁴⁵ Ove podatke moraju dostaviti službama na njihov zahtjev. Na osnovu *Direktive Evropske unije o zadržavanju podataka* iz 2006. godine⁴⁶, ovi zakoni su uveli i obavezu operatera da zadržavaju podatke o komunikacijama svih svojih korisnika. Riječ je o podacima koji otkrivaju izvor i odredište komunikacije, vrijeme njenog početka, trajanja i završetka, lokaciju i vrstu korišćene opreme, kao i vrstu komunikacije, bez otkrivanja njenog sadržaja.⁴⁷ U Hrvatskoj je propisan period zadržavanja od godinu dana. Isto važi u Holandiji za mobilnu i fiksnu telefoniju, dok je period za pristup internetu, elektronskoj pošti i internet telefoniji duplo kraći.⁴⁸ Operater garantuje bezbjednost, integritet i kvalitet ovih podataka.⁴⁹

41 Član 38 ZSOS-a.

42 Narodne novine broj 73/08, 90/11, 133/12, 80/13 i 71/14, članovi 108–110.

43 Narodne novine broj 64/08 i **76/13**.

44 Telecommunicatiewet, Staatsblad 610, 1998., sa posljednjim izmjenama 2015. godine, članovi 13.1–13.10.

45 Prema članu 33 UEK, ova obaveza uključuje i čuvanje podataka o pojedinim telekomunikacijskim i pripejd priključcima, a baza identifikacionih podataka mora redovno da se ažurira. Prema članu 13.4(2) holandskog ZT-a čuvaju se: ime i adresa korisnika, njegov broj i vrsta usluge koju koristi. Takođe, član 29 ZOBS-a.

46 „Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.” *OJ L* 105, 13. 4. 2006.

47 Član 110 ZEK-a i članovi 21–26 UEK-a. Za Holandiju član 13.2a Zakona o telekomunikacijama uz Aneks. Takođe član 28 ZOBS-a.

48 Član 13.2a(3) holandskog ZT-a.

49 Član 6 UEK-a, koji propisuje i da svi zaposleni koji sa ovim podacima rade moraju proći bezbjednosnu provjeru. Za Holandiju član 13.5(2) ZT-a.

Podaci se zadržavaju kako bi se bezbjednosno-obavještajnim službama omogućio pristup radi zaštite nacionalne bezbjednosti, kao i drugim nadležnim organima radi borbe protiv teških krivičnih djela.⁵⁰ Ova posebna mjera tajnog prikupljanja podataka smatra se manje intruzivnom, tako da je u obje zemlje dovoljno da direktor službe uputi nalog operateru.⁵¹ Samo u Holandiji je sadržaj ovog naloga zakonski propisan: navode se broj, podaci o imenu i prebivalištu lica, odnosno podaci o nazivu i sjedištu organizacije o kojoj jer riječ, opis podataka koji se traže i obuhvaćen vremenski period.⁵² S druge strane, samo hrvatski ZEK izričito zahtijeva uništavanje neiskorištenih podataka po isteku perioda zadržavanja.⁵³ Pored toga, u Hrvatskoj se od operatera može tražiti i da dostave podatke o svim sredstvima komunikacije, koja su se pojavljivala na određenoj lokaciji u posljednjih 48 sati, čak i ako ta sredstva za to vrijeme nisu korišćena.⁵⁴

Sud pravde EU oglasio je u aprilu 2014. ništavom *Direktivu o zadržavanju podataka* zbog nepreciznosti prilikom određenja obima i svrhe njene primjene, predviđenog perioda zadržavanja, ali i nedovoljnih garancija bezbjednosti i integriteta podataka.⁵⁵ Poništenje Direktive nije automatski ukinulo nacionalne zakone koji su je sprovodili, a pošto zakonske izmjene nisu uslijedile ni u Hrvatskoj ni u Holandiji, nije jasno ko će preuzeti obavezu Evropske komisije o godišnjem prikupljanju statističkih podataka o primijenjenim mjerama radi evaluacije. Ova statistika, inače, sadrži podatke o broju ispunjenih i odbijenih zahtjeva za pristup zadržanim podacima, kao i vrijeme koje je proteklo od dana zadržavanja podataka do podnošenja takvog zahtjeva operateru.⁵⁶

50 Pristup zadržanim podacima omogućen je i drugim tijelima, ovlaštenim hrvatskim i holandskim zakonima o krivičnom postupku, ali mi ćemo se u ovoj analizi zadržati samo na radu bezbjednosno-obavještajnih službi. Treba ipak napomenuti da, npr. u Hrvatskoj, tek 10% zahtjeva za pristup dolazi od ovih službi. Vidjeti: Tuđman, M. „O iskustvima parlamentarnog nadzora i funkcionalnosti izvještajnog sustava Republike Hrvatske”, Zagreb, 2013. Tekst dostupan na: <<http://www.hkv.hr/vijesti/dokumenti/22736-rasclamba-koju-je-prof-dr-sc-m-tudman-2013-poslao-josipovicu-i-milanovicu.html>> 25. 4. 2016.

51 Član 28 ZOBS-a, član 38 ZSOS-a.

52 Član 28 ZOBS-a.

53 Član 109(5)4 ZEK-a.

54 Član 19(6) ZSOS-a, član 27 UEK-a.

55 *Digital Rights Ireland v. Ireland & Seitlinger et al.* Judgement of the Court of Justice of the European Union, C293/12 and C594/12, 8.4.2014., para. 57–66.

56 Član 110(4) hrvatskog ZEK-a i član 40.a UEK-a, te član 13.9 holandskog Zakona o telekomunikacijama.

Položaj i uloga specijalizovanih tijela

U Hrvatskoj i Holandiji obje bezbjednosno-obavještajne službe imaju specijalizovano tijelo, koje za njih obavlja tajni nadzor elektronskih komunikacija, mada je način njihovog uređenja u ove dvije zemlje bitno drugačiji. Zajednička sigint sajber jedinica (JSCU) postoji od 2014. godine na osnovu sporazuma potpisanog između AIVD-a i MIVD-a. Sačinjena je od njihovih zaposlenika. Njen zadatak je da prikuplja i filtrira podatke, obezbijedi pristup njima, te pruži službama stručnu pomoć u svojoj oblasti. Iako svaka od službi ulaže svoju opremu i sredstva, te snosi odgovornost za podatke koje je sama tražila, kao i za njihovo arhiviranje, prikupljeni podaci unutar JSCU stoje na raspolaganju objema službama u skladu sa njihovim nadležnostima.

U Hrvatskoj je status Operativno-tehničkog centra (OTC) zakonski regulisan.⁵⁷ Kao dio bezbjednosno-obavještajnog sistema, on predstavlja posrednika između službi i operatera u slučajevima tajnog nadziranja komunikacija. Ova funkcija se ostvaruje ugradnjom odgovarajuće tehničke opreme i softvera u telekomunikacijski sistem operatera. Operativno-tehnički centar ima trajan i direktan pristup objektima i tehničkoj opremi operatera, i može samostalno da primjenjuje predviđene mjere nadzora. Druga njegova uloga je da nadzire kako operateri ispunjavaju svoje zakonske obaveze⁵⁸ i da li poštuju tehničke standarde koje su propisale SOA i VSOA, a može zahtijevati i da Hrvatska regulatorna agencija za mrežne djelatnosti sprovede nad operaterima postupak inspekcijskog nadzora. Zakon ne spominje obavezu OTC-a da vodi evidencije, već su operateri dužni da mu, na njegov zahtjev, dostavljaju podatke o sprovedenim postupcima, broju primljenih zahtjeva, pravnom osnovu tih zahtjeva i vrsti podataka koji su dostavljeni.⁵⁹ Pristup podacima o aktiviranim mjerama takođe mora biti u svakom trenutku zajamčen, kako za OTC, tako i za nadležna nadzorna i istražna tijela.

⁵⁷ Članovi 18–22 ZSOS-a, te članovi 108–110 ZEK-a.

⁵⁸ U članu 11(2) UEK-a precizirano je da se nadzor nad operaterima sprovodi jednom godišnje, a po potrebi i češće. Operativno-tehnički centar potom izdaje Potvrdu o ispravnosti funkcije tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa (član 14 UEK-a).

⁵⁹ Član 108(9) ZEK-a.

UNUTRAŠNJA KONTROLA

Unutrašnja kontrola nije zakonski predviđena ni u Holandiji ni u Hrvatskoj. U holandskom ZOBS-u nije uopšte spominuta, dok je hrvatski ZSOS izričito prepušta podzakonskim aktima, koji su uglavnom označeni kao povjerljivi.

Prema zvaničnom sajtu AIVD-a, zadatak unutrašnje kontrole obavlja njeno centralno osoblje.⁶⁰ Ministarstvo odbrane, u sklopu kojeg djeluje MIVD, ima posebnu jedinicu za finansije i kontrolu, ali se ona uglavnom bavi finansijskim nadzorom, a Generalni inspektor za Oružane snage djeluje kao posrednik u (radnim) sporovima zaposlenih sa MIVD-om.⁶¹ Nacrt novog ZOBS-a iz 2015. godine u članovima 114–120 predviđa prvi put i zaštitu za uzbunjivače, odnosno za zaposlenike službi koji uoče nepravilnosti u postupanju svojih kolega.

U zvaničnoj brošuri o SOA, osim unutrašnjeg (finansijskog) revizora koji odgovara direktoru, spominje se i Jedinica za protivobavještajnu zaštitu i nadzor, koja vrši i nadzor nad zakonitošću rada Službe i njenih zaposlenih, te se brine o zaštiti ugleda SOA i sukobu interesa koji može proizaći iz aktivnosti zaposlenih van radnog vremena.⁶² Takođe, Uredbom o ustrojavanju disciplinskih sudova SOA iz 2006. godine osnivaju se prvostepeni i drugostepeni disciplinski sudovi za povrede službene i radne dužnosti. Disciplinski sudovi su uredbama iste godine predviđeni i za VSOA i UVNS.

Vojna sigurnosno-obavještajna agencija nalazi se u sklopu Ministarstva odbrane, koje kao kontrolna tijela ima Samostalni odjel za unutrašnju reviziju i Inspektorat obrane.⁶³ Odjel obavlja finansijsku reviziju, ocjenjujući pritom zakonitost i efikasnost utrošenih sredstava Ministarstva⁶⁴, dok se Inspektorat obrane ne bavi VSOA⁶⁵.

60 Opšta obavještajno-bezbjednosna služba (AIVD) sastoji se iz centralnog osoblja i tri direktorata – obavještajnog direktorata, operativnog direktorata i direktorata za bezbjednosne provjere i poslovnu administraciju. Vidjeti: Zvanični sajt AIVD-a <<https://english.aivd.nl/about-aivd/contents/the-aivd-who-we-are>> 9. 4. 2016.

61 Zvanični sajt holandskog Ministarstva odbrane. <<https://www.defensie.nl/organisatie/bestuur/staf/inhoud/eenheden/mivd>> 9. 4. 2016.

62 Brošura SOA iz 2014, str. 12 i 37. Dostupno na: <https://www.soa.hr/UserFiles/File/pdf/JAVNI-DOKUMENT_web.pdf> 15. 1. 2016. U SOA *Katalogu informacija* iz 2013. godine podaci o unutrašnjoj organizaciji i redu ove službe naznačeni su kao povjerljivi i nedostupni javnosti mada se u poglavlju o normativnom okviru u istom dokumentu nabrajaju Uredba o unutarnjem ustrojstvu SOA i Pravilnik o unutarnjem redu SOA. Dostupno na: <<https://www.soa.hr/UserFiles/File/pdf/Katalog-informacija-08-03-2013.pdf>> 15. 1. 2016.

63 Član 3 *Uredbe o unutarnjem ustrojstvu Ministarstva obrane*, Narodne novine, broj 26/12, 112/12, 94/14 i **93/15**

64 Član 19 *Uredbe*.

65 Član 157 *Uredbe*.

SPOLJNA KONTROLA I NADZOR

Spoljnu kontrolu vrše izvršni, zakonodavni i sudski organi, kao i nezavisne nadzorne institucije i tijela specijalizovana za nadzor nad bezbjednosno-obavještajnim službama. Izvršni nadzor u Holandiji vrši Vlada, odnosno nadležni ministri, a u Hrvatskoj, pored Vlade, i predsjednik Republike. U obje je zemlje parlamentarni nadzor nadasve zadatak nadležnog parlamentarnog odbora, mada ga formalno vrši i plenum. Sudska kontrola postoji kroz obavezu pribavljanja prethodnog sudskog odobrenja za primjenu pojedinih posebnih mjera. Obje zemlje imaju i specijalizovana tijela koja nadziru rad službi. U Holandiji je to Nadzorna komisija za obavještajne i bezbjednosne službe (CTIVD), koja je nezavisno ekspertsko tijelo. U Hrvatskoj stručni nadzor vrši Ured Vijeća za nacionalnu sigurnost (UVNS), koji je i sam dio bezbjednosno-obavještajnog sistema i podređen izvršnoj vlasti. Predviđeno je, međutim, i Vijeće za građanski nadzor sigurnosno-obavještajnih agencija, sa poluekspertskim sastavom i statusom radnog parlamentarnog tijela. Dok holandski CTIVD nadzire sva lica koja sprovode ZBOS, dotle je nadležnost hrvatskog Vijeća ograničena samo na službe, dok jedino UVNS vrši nadzor nad Operativno-tehničkim centrom. Među nezavisnim državnim institucijama, nadležnost nadzornog tijela za zaštitu ličnih podataka proteže se na službe samo u Hrvatskoj, a zaštitnik građana ih u svom djelokrugu nadzire u obje zemlje. Oba zakonodavstva propisuju i obavezu obavještavanja lica, na njihov zahtjev, o posebnim mjerama koje su nad njima sprovedene, a u Holandiji čak i samoinicijativno.

Izvršni nadzor

Nadležni ministri u Holandiji odgovorni su za rad službi i rješavaju po žalbama na njihovo postupanje. Uredba o rješavanju po žalbama u AIVD-u iz 2007.⁶⁶ predviđa da žalbe prima „koordinator za žalbe“, koji je zaposleni AIVD-a, a kome je taj zadatak odredio generalni direktor. Ovo lice registruje sve žalbe i one se anonimno objavljuju u godišnjem izvještaju AIVD-a. U roku od dvije sedmice žalbe se proslijeđuju Nadzornoj komisiji za obavještajne i bezbjednosne službe (CTIVD) i traži se mišljenje ovog tijela prije donošenja odluke. Moguće je da o žalbama odlučuje generalni sekretar MUP-a, ako nije riječ o ponovljenoj žalbi, političkom ili društvenom pitanju suštinske i/ili osjetljive prirode ili ako se odlučuje suprotno mišljenju CTIVD-a. U Hrvatskoj izvršni nadzor nije preciziran i uglavnom se oslanja na stručni nadzor koji vrši UVNS.

66 Besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 6 september 2007, nr. 2918470/01, tot vaststelling van de Klachtregeling AIVD. Dostupno na: <<http://wetten.overheid.nl/BWBR0022497/2007-09-14>> 22. 2. 2016.

Parlamentarni nadzor

Parlamentarni nadzor u Hrvatskoj vrši Sabor neposredno ili preko nadležnog odbora – Odbora za unutarnju politiku i nacionalnu sigurnost (Odbor). Nadzor je usmjeren na provjeru zakonitosti rada službi, tako da ne obuhvata razmatranje godišnjih planova rada SOA i VSOA, niti njihovo poređenje sa godišnjim izvještajima radi moguće procjene efikasnosti ili svrsishodnosti.⁶⁷ Odborom predsjedava predstavnik najzastupljenije opozicione stranke u Saboru, što je izričito zakonski predviđeno⁶⁸ i služi kao dodatno jamstvo efikasne kontrole. Sabor može tražiti i izvještaje o primjeni posebnih mjera tajnog prikupljanja podataka, kako od službi, tako i od predsjednika Vrhovnog suda. Ostali dijelovi bezbjednosno-obavještajnog sistema Hrvatske, poput OTC-a, ZSIS-a i UVNS-a, ostaju van parlamentarnog nadzora. Sabor, međutim, može naložiti UVNS-u da obavi nadzor nad radom OTC-a, o čemu će naknadno primiti izvještaj samo ukoliko su nadzorom utvrđene nepravilnosti.⁶⁹

Donji dom Parlamenta Kraljevine Holandije ima Odbor za obavještajne i bezbjednosne službe (*Commissie voor de Inlichtingen- en Veiligheidsdiensten – CIVD*), koji, za razliku od Odbora za odbranu i Odbora za unutrašnje poslove, jedini može da prima i povjerljive podatke. Međutim, poslanici su, kao i u Hrvatskoj, oslobođeni obaveze da prođu bezbjednosnu provjeru.⁷⁰ Članovi CIVD-a isključivo su čelnici svih poslaničkih grupa⁷¹ i o svojim aktivnostima godišnje izvještavaju parlament.⁷² Praksa, međutim, pokazuje da parlamentarni nadzor nad AIVD-om uglavnom preuzima Odbor za unutrašnje poslove, koji razmatra njegove godišnje i javne izvještaje, kao i teme u vezi sa AIVD-om koje uživaju medijsku pažnju, dok se CIVD-u ostavljaju samo oblasti koje zahtijevaju povjerljivost.⁷³

67 M. Tudman, op.cit.

68 Član 105(4) ZSOS-a.

69 Član 109 ZSOS-a.

70 Razlog je insistiranje na razdvajanju grana vlasti. Verhoeven, N. „Parliamentary and specialised oversight of security and intelligence agencies in the Netherlands”, u: Wills, A. Vermeulen, M. „Parliamentary Oversight of Security and Intelligence Agencies in the European Union”, Civil Liberties, Justice and Home Affairs Committee of the European Parliament, Brussels, 2011, str. 282.

71 Vidjeti član 22 Poslovnika Donjeg doma holandskog Parlamenta. Dostupno na: <http://www.parlement.com/id/vh8lnhrqszxv/reglement_van_orde_tweede_kamer> 5. 5. 2016.

72 Zvanični sajt Donjeg doma Parlamenta. Dostupno na: <<http://www.tweedekamer.nl/kamerleden/commissies/iv>> 20. 1. 2016.

73 Verhoeven, N. op.cit., str. 282.

Specijalizovana nadzorna tijela

Holandska Nadzorna komisija za obavještajne i bezbjednosne službe (*Commissie van Toezicht betreffende de Inlichtingen-en Veiligheidsdiensten – CTIVD*) predstavlja ekspertsko tijelo koje nadzire zakonitost postupanja službi, savjetuje nadležne ministre o pitanjima iz svoje oblasti i davanjem neobavezujućeg mišljenja učestvuje u opisanom postupku po žalbi na rad službi. Ona ima tri člana koji se kolektivno imenuju kraljevskim ukazom, na osnovu prijedloga nadležnih ministara. Članovi moraju biti holandski državljani, visoko obrazovani pravnici i moraju biti izvan sukoba interesa.⁷⁴ U složenom postupku njihovog izbora ključnu ulogu igraju nadležni ministri. Bez obzira na to što član 65 predviđa da listu kandidata sastavljaju parlament i drugi akteri (predsjednik Vrhovnog suda, Ombudsman), ministri mogu tražiti novu listu ako im postojeća ne odgovara. Oni imaju pravo i da zajedničkom odlukom suspenduju člana Komisije zbog razloga predviđenih zakonom.⁷⁵ Nedovoljna nezavisnost Komisije od nadležnih ministara ogleda se i u tome što se na osnovu njihove zajedničke preporuke imenuju i članovi sekretarijata, koje ovom tijelu pomaže da obavlja predviđene zadatke.

Službe, nadležni ministri, koordinator službi i svako ko učestvuje u primjeni ZOBS-a⁷⁶, uključujući u to i JSCU, podložni su nadzoru CTIVD-a i dužni da sarađuju sa njim, nadasve dostavljanjem traženih podataka, kao i saslušanjem u svojstvu svjedoka ili eksperta, ali i obezbjeđenjem pristupa prostorijama Nadzorna komisija za obavještajne i bezbjednosne službe ovlaštena je da sprovodi istrage o primjeni ovog Zakona, te ima neposredan pristup svim podacima koji se u sklopu primjene obrađuju, uključujući u to i podatke označene različitim stepenima povjerljivosti.⁷⁷ U tu svrhu ima obezbijeđen sopstveni prostor i računare u prostorijama službi⁷⁸, a njegovi članovi moraju proći bezbjednosnu provjeru. Po završetku istrage ovo tijelo sastavlja javni izvještaj, koji prvo dostavlja nadležnom ministru. Ovaj ministar potom u roku od šest sedmica šalje izvještaj, zajedno sa svojim odgovorom, oboma domovima parlamenta.⁷⁹ Za razliku od sastanaka CTIVD-a, njegov Godišnji izvještaj u potpunosti je dostupan javnosti. Komisija, međutim, u svojim istragama može da kontroliše samo zakonitost rada službi. Ona se ne bavi ocjenom efikasnosti mjera koje službe sprovode i ne može ih spriječiti niti zaustaviti. Njene odluke nisu obavezujuće, pa čak i onda kada utvrdi da nezakonito postupanje postoji, nema ovlaštenje

74 Član 65(7) ZOBS-a. Zakon ne daje spisak funkcija sa kojim je članstvo u Komisiji nespojivo, već uopšteno isključuje kao nepoželjne one koje mogu dovesti u pitanje nepristrasnost i nezavisnost Komisije ili bar povjerenje da ona tako djeluje.

75 Na primjer, ako je član Komisije privremeno lišen slobode ili ako je oglasio bankrot. Suspendizija traje tri mjeseca, ali se može više puta produžiti za još toliko. Vidjeti: član 67 ZOBS-a.

76 Tijela koja mogu učestvovati u sprovođenju ZOBS-a nabrojana su u članu 60 ovog Zakona.

77 Član 73 ZOBS-a. Formulacija ovog člana navodi na zaključak da CTIVD može vršiti nadzor i u realnom vremenu, jer podaci koji su mu dostupni nisu ograničeni na okončane mjere.

78 Verhoeven, N., op.cit., str. 284.

79 Na primjer, 2014. godine objavljen je *Izvještaj br. 38* o rezultatima istrage o nadzoru AIVD-a i MIVD-a nad telekomunikacijama.

da naredi obustavu takvog postupanja niti uništenje nezakonito prikupljenih podataka. Ona jedino prilikom savjetovanja nadležnih ministara, na njihov zahtjev ili samoinicijativno, može da se osvrne i na svrsishodnost, efikasnost i druge teme iz svoje stručne oblasti.

Za razliku od CTIVD-a, hrvatsko Vijeće za građanski nadzor sigurnosno-obavještajnih agencija vodi se kao parlamentarno tijelo. Sabor utvrđuje program njegovog rada i bira njegove članove iz reda uglednih građana na obnovljiv mandat od četiri godine. Poluekspertski karakter Vijeću daje zakonski uslov da u njegovom sedmočlanom sastavu bude bar po jedan diplomirani politolog, pravnik i inženjer elektrotehnike⁸⁰, s obzirom na to da se nadzire i zakonitost primjene posebnih mjera, kojima se zadire u osnovna prava i slobode građana, često sredstvima visoke tehnologije. Ova lica ne mogu istovremeno biti članovi užeg rukovodstva političkih stranaka, te ne smiju učestvovati u stranačkim aktivnostima. Drugim riječima, mogu biti neaktivni obični članovi stranke. Vijeće ima pravo na uvid u dokumenta službi, kao i na obavljanje razgovora sa čelnicima i službenicima službi, pa zato njegovi članovi moraju proći bezbjednosnu provjeru. Ono prima predstavke građana i postupa po njima. Predstavke mogu da podnesu i državna tijela i pravna lica ako primijete nepravilnosti u radu službi. Fokus nadzora je na poštovanju Ustavom zajemčenih građanskih prava i sloboda. Vijeće dva puta godišnje Saboru dostavlja izvještaj o svom radu, a o rezultatima nadzora koji ukazuju na nezakonitost rada službi obavještava prvo Odbor, a potom i predsjednika RH, predsjednika Sabora, premijera i javnog tužioca.⁸¹

Uloga Vijeća kao nosioca građanskog nadzora umanjuje se njegovom potpunom zavisnošću od nadležnog saborskog Odbora, bez čijeg odobrenja ne može ni javno istupati, kao i izuzećem OTC-a iz njegovog nadzora. Takođe, Vijeće nema svoju internet stranicu, postupak za podnošenje predstavke nije objašnjen ni na zvaničnom sajtu Sabora, a posljednji izvještaj o radu, čak i u sažetoj formi, objavljen je 2010. godine. Najzad, u trenutku pisanja ove analize Vijeće već više od šest mjeseci nije aktivno, pošto novi članovi nisu izabrani još od isteka mandata prošlog sastava u oktobru 2015. godine.⁸²

Zakonom predviđen stručni nadzor u Hrvatskoj nije nezavisan, a ni sasvim spoljni, jer je prepušten Uredu Vijeća za nacionalnu sigurnost kao dijelu bezbjednosno-obavještajnog sistema. Za razliku od građanskog nadzora, koje obuhvata samo rad SOA i VSOA, UVNS nadzire i rad Operativno-tehničkog centra. Takođe, on prati ne samo zakonitost rada, uključujući u to i primjenu posebnih mjera već nadzire i ostvarivanje propisanih ciljeva, efikasnost i svrsishodnost, upotrebu finansijskih sredstava, ali i koordinaciju i međusobnu saradnju službi, te njihovu saradnju

80 Član 110(3) ZSOS-a.

81 Članovi 110–114 ZSOS-a, kao i *Odluka Hrvatskog sabora o Vijeću za građanski nadzor sigurnosno-obavještajnih agencija*, 27. 4. 2007.

82 Žapčić, Andreja. „Tko će se javiti za članstvo u Vijeću za građanski nadzor sigurnosnih službi“, tportal.hr, 2. 3. 2016. Dostupno na: <<http://www.tportal.hr/vijesti/hrvatska/417728/Tko-ce-se-javiti-za-clanstvo-u-Vijecu-za-gradanski-nadzor-sigurnosnih-sluzbi.html>> 10. 5. 2016.

sa inostranim službama. Radi toga, može ostvariti uvid u dokumenta službi, ali i obavljati razgovore sa njihovim direktorima i drugim zaposlenicima. Nadzor koji vrši UVNS može naložiti predsjednik RH, predsjednik Vlade RH, predsjednik Hrvatskog sabora, Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora, te načelnik UVNS-a. O rezultatima nadzora tokom kog su ustanovljene nepravilnosti u radu službi izvještavaju se predsjednik i premijer, dok se Sabor i njegov nadležni Odbor izvještavaju samo ako su oni taj nadzor naložili.⁸³ Predsjedniku i premijeru UVNS dostavlja i godišnje izvještaje o svom radu i o obavljenim poslovima nadzora, a Saboru i nadležnom Odboru dostavlja samo potonje.⁸⁴

Nadzor nad ZSIS-om nije posebno predviđen, već je sadržan jedino u obavezi direktora ovog tijela da UVNS-u šalje izvještaje o svom radu, a Zakonom nije čak određeno ni u kojim vremenskim intervalima.⁸⁵ Jedino je UVNS nadležan da nadzire rad OTC-a, ali je od većeg značaja da se nadzor nad njim proširi⁸⁶, s obzirom na to da je u ovom tijelu koncentrisana primjena posebnih mjera tajnog nadzora nad komunikacijama.

Nadzor koji vrše nezavisne državne institucije

Nadzor nad bezbjednosno-obavještajnim službama spada i u nadležnosti institucije zaštitnika građana u obje zemlje. Pučki pravobranitelj u Hrvatskoj nadzire zaštitu ustavnih i zakonskih prava građana u postupanju SOA i VSOA, te o tome podnosi izvještaj Saboru.⁸⁷ Holandskom Nacionalnom ombudsmanu je ZOBS izričito dodijelio ulogu drugostepene žalbene instance. Ombudsman rješava po žalbama na postupanje bilo kog upravnog organa koji sprovodi ovaj Zakon, ali tek nakon što je iscrpljena prethodno opisana prvestepena žalbena procedura.⁸⁸ Odluka Ombudsmana po žalbi nije obavezujuća, ali se dostavlja i nadležnom ministru, a sa njegovim komentarom i oboma domovima parlamenta.⁸⁹ Za razliku od hrvatske Agencije za zaštitu

83 Članovi 106–109 ZSOS-a.

84 Član 8 ZSOS-a.

85 Član 15(3) ZSOS-a.

86 Saborski Odbor za unutrašnju politiku i nacionalnu bezbjednost podnio je 2009. godine, a ponovo u martu 2016, prijedlog za autentično tumačenje članova ZSOS-a koji se bave građanskim nadzorom (čl. 110–112), sa stavom da pravo Vijeća da nadzire OTC proizilazi iz njegovog ovlaštenja da nadzire službe. Naime, iako je OTC zasebno tijelo, službe su njegov nalogodavac u primjeni posebnih mjera, te Odbor smatra da je postojeće tumačenje Zakona preusko. Vlada je dala negativno mišljenje o prijedlogu. Relevantna dokumenta su dostupna na: <<https://vlada.gov.hr/UserDocsImages//Sjednice/2016/15%20sjednica%20Vlade//15%20-%209.7.pdf>> 2. 5. 2016.

87 Član 105 ZSOS-a. Međutim, na zvaničnoj internet stranici nema posebnih izvještaja o nadzoru nad službama, niti se one spominju u godišnjim izvještajima o radu Pučkog pravobranitelja.

88 Čl. 83 ZOBS-a.

89 Čl. 84 ZOBS-a.

osobnih podataka⁹⁰, nadležnost istovrsnog **nezavisnog nadzornog organa** u Holandiji ne proteže se na bezbjednosno-obavještajne službe⁹¹.

Izvještavanje, obavještavanje i transparentnost

Još jedan vid nadzora ogleda se u obavezi službi da sastavljaju **godišnji izvještaj o radu**. U Holandiji nadležni ministri dostavljaju ove izvještaje samo Parlamentu, a u Hrvatskoj ih direktori službi šalju dodatno i predsjedniku Republike, premijeru i načelniku UVNS-a. U obje zemlje predviđeni su i vanredni izvještaji, koji se po potrebi dostavljaju na iste adrese. Sadržaj ovih izvještaja zakonski je samo uopšteno naznačen. U Holandiji je posvećen oblastima posebne pažnje u prethodnoj i narednoj godini, a u Hrvatskoj važnim prikupljenim podacima i procjeni bezbjednosne situacije.⁹² Dakle, ne zahtijeva se i navođenje broja primijenjenih posebnih mjera, procenat njihovog uspješnog korišćenja i slično. Takođe, ni ZOBS ni ZSOS ne bave se razlozima ili posljedicama eventualnog odbijanja izvještaja, što se nedavno i desilo u nadležnom Odboru Hrvatskog sabora.⁹³

U skladu sa evropskim zakonodavstvom u oblasti zaštite ličnih podataka, hrvatski i holandski zakoni uređuju i **obavezu obavještavanja pojedinaca**, na njihov zahtjev, o podacima koji su o njemu posebnim mjerama prikupile bezbjednosno-obavještajne službe, kao i pravo tih pojedinaca na pristup i ispravku tih podataka.⁹⁴ Holandski zakonodavac je ovome posvetio veću pažnju, a od 2007. uveo je i obavezu samoinicijativnog obavještavanja pojedinaca.

U Holandiji o zahtjevu pogođenog pojedinca odlučuje nadležni ministar. Odgovor na zahtjev treba da uslijedi u roku od tri mjeseca, a može da se odgodi za još četiri sedmice, uz blagovremeno i pismeno obrazloženje. Zahtjev će biti odbijen ako se odnosi na podatke koji su prikupljeni tokom prethodnih pet godina i/ili su važni za aktuelnu istragu. U Hrvatskoj će zahtjev biti odbijen ako bi se odgovorom ugrozilo izvršenje zadataka službe, bezbjednost drugih ili

90 Članovi 32 i 33 Zakona o zaštiti osobnih podataka, „Narodne novine“, br. 103/03, 118/06, 41/08, 130/11. Član 3 ovog Zakona propisuje njegovo opšte važenje za voditelje zbirke ličnih podataka, bez ikakvih izuzetaka ili specifičnosti za bezbjednosno-obavještajne službe.

91 Član 2(2)b holandskog Zakona o zaštiti ličnih podataka isključuje bezbjednosne službe iz svog domena primjene. Nezvaničan prevod Zakona na engleski jezik dostupan je na: <https://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf> 20. 3. 2016.

92 Član 8 holandskog ZOBS-a, član 55 hrvatskog ZSOS-a.

93 Krajem februara je odbijen godišnji izvještaj SOA. Vidjeti: <<http://www.jutarnji.hr/palo-izvjesce-sefa-soa-e-presudila-strenja-linic/1528524/>> 5. 5. 2016. Nekoliko sedmica kasnije odbijeni su godišnji izvještaj VSOA i izvještaj UVNS-a o izvršenom stručnom nadzoru. Vidjeti: <<http://www.vecernji.hr/hrvatska/odbor-za-unutarnju-politiku-i-nacionalnu-sigurnost-odbio-izvjesca-vojne-soa-e-te-ureda-vijeca-za-nacionalnu-sigurnost-1067210>> 5. 5. 2016.

94 Članovi 47–57 holandskog ZOBS-a, član 40 hrvatskog ZSOS-a.

nacionalna bezbjednost i nacionalni interes. Kada je riječ o posljednjem razlogu, prilično široko definisanom, opravdano je na dostupnost ovih podataka čekati i do deset godina od preduzimanja mjere, tako da se obaveza obavještanja praktično obesmišljava.

U Holandiji su, pored toga, nadležni ministri dužni da, pet godina nakon primjene posebne mjere⁹⁵ i naknadno na godišnjem nivou, pregledaju evidenciju službe i razmatraju da li je moguće poslati pogođenom licu izvještaj o primijenjenoj mjeri koja se na njega odnosi. Ako to nije moguće, obavještava se CTIVD uz obrazloženje. Izvještaj sadrži podatke o pogođenom licu, vrsti mjere koja je primijenjena, trajanju primjene, identitetu lica koje ju je odobrilo i datum odobrenja. Obaveza obavještanja prestaje ako se utvrdi da to „razumno nije moguće”⁹⁶ i da može otkriti izvore službe, njene posebne metode i saradnike, ili ako bi to ozbiljno oštetilo odnose sa drugim državama i međunarodnim organizacijama. Ova obaveza odgađa se u slučaju da je time aktuelna istraga ugrožena. Nadzorna komisija za obavještajne i bezbjednosne službe sprovodi nadzor nad vršenjem ove obaveze kroz povremene kontrole nasumično izabranih slučajeva.

Na kraju, kada je riječ o **transparentnosti**, treba napomenuti da su u tom smjeru veliki iskorak napravile AIVD i SOA, na čijim je internet stranicama moguće naći njihovu unutrašnju organizaciju, pratiti novosti i javne izvještaje o radu, kao i relevantne pravne i strateške akte. Zvanični sajt UVNS-a je, takođe, dosta informativan. Podaci o MIVD-u sa godišnjim izvještajima nalaze se na sajtu Ministarstva odbrane, dok je VSOA samo spomenuta na sajtu hrvatskog Ministarstva obrane kao njegova ustrojstvena jedinica. Zajednička sigint sajber jedinica i Operativno-tehnički centar, kao specijalizovana tijela, takođe nemaju svoje internet stranice, te je njihov rad sasvim netransparentan.

95 Ova obaveza se ne odnosi na sve mjere tajnog nadzora nad komunikacijama, već samo na presretanje pošiljki, kablovskih komunikacija i odabir snimljenih nekablovskih komunikacija. Pristup zadržanim elektronskim podacima je, dakle, izostavljen. Vidjeti: član 34 ZOBS-a.

96 Član 34(7) ZOBS-a.

RELEVANTNI PRAVNI OKVIR

Hrvatska

Zakon o sigurnosno-obavještajnom sustavu, Narodne novine br. 79/06, 105/06.

Zakon o elektroničkim komunikacijama, Narodne novine br. 73/08, 90/11, 133/12, 80/13 i 71/14.

Zakon o zaštiti osobnih podataka, Narodne novine br. 103/03, 118/06, 41/08, 130/11.

Zakon o Pučkom pravobranitelju, Narodne novine 76/12.

*Uredba o obvezama iz područja nacionalne sigurnosti za pravne i fizičke osobe u telekomunikacijama, Narodne novine br. 64/08 i **76/13**.*

Poslovnik Hrvatskog sabora, Narodne novine br. 81/13.

Odluka Hrvatskog sabora o Vijeću za građanski nadzor sigurnosno-obavještajnih agencija, 27. 4. 2007.

Holandija

*Zakon o obavještajnim i bezbjednosnim službama (Wetop deinlichtingen-en veiligheidsdiensten), **Staatsblad van het Koninkrijk der Nederlanden 148 2002, 574 2006.***

Zakon o telekomunikacijama (Telecommunicatiewet), Staatsblad 610, 1998, sa posljednjim izmjenama 2015. godine

Zakon o zaštiti ličnih podataka (Wet bescherming persoonsgegevens), Staatsblad 320, 6. 7. 2000, sa posljednjim izmjenama 2015. godine

Sporazum između AIVD-a i MIVD-a o Zajedničkoj sigint sajber jedinici od 3. jula 2014. godine. (Convenant AIVD – MIVD inzake de Joint Sigint Cyber Unit De Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie)

Uredba o rješavanju po žalbama u AIVD-u (Besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties tot vaststelling van de Klachtregeling AIVD), 6. 9. 2007, nr. 2918470/01.

Poslovnik Donjeg doma holandskog Parlamenta (*Reglement van Orde van de Tweede Kamer der Staten-Generaal*), Kamerstukken II 1991/92 en 1992/93, 22590, handelingen II 1992/93, nrs. 31 en 33, sa posljednjim izmjenama 2016.

LITERATURA

Cvrtila, V. „Razvoj i nadzor sigurnosno-obavještajnog sustava u Republici Hrvatskoj”, DCAF. <http://www.dcaf.ch/content/download/104962/1617971/version/2/file/croatia_cro1.pdf> 20. 2. 2016.

„Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States’ legal frameworks”, European Union Agency for Fundamental Rights, Luxembourg, 2015.

Tudman, M. „O iskustvima parlamentarnog nadzora i funkcionalnosti izvještajnog sustava Republike Hrvatske”, Zagreb, 2013. <<http://www.hkv.hr/vijesti/dokumenti/22736-rasclamba-koju-je-prof-dr-sc-m-tudman-2013-poslao-josipovicu-i-milanovicu.html>> 25. 4. 2016.

Wiebes, C. „Oversight or Aftersight? Democratic control over Netherlands Security community”, in: Schmidt, W., Poppe, U. et. al. (eds), *Geheimhaltung und Transparenz: Demokratische Kontrolle der Sicherheitsdiensten in internationalen Vergleich*, LIT Verlag, Berlin 2007, pp. 106–128.

Wills, A. Vermeulen, M. „Parliamentary Oversight of Security and Intelligence Agencies in the European Union”, Civil Liberties, Justice and Home Affairs Committee of the European Parliament, Brussels, 2011.

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

351.86(492)

351.86(497.5)

ПЕЈИЋ, Јелена, 1991-

Bezbednosno-obavještajni sistemi u državama članicama Evropske unije :
primjeri Holandije i Hrvatske / Jelena Pejić. - Beograd : Beogradski centar
za bezbednosnu politiku, 2016 (Beograd : Unagraf). - 29 str. ; 25 cm

Tiraž 100. - Napomene i bibliografske reference uz tekst. - Bibliografija:
str. 29.

ISBN 978-86-6237-131-7

a) Безбедносни сектор - Холандија b) Безбедносни сектор - Хрватска
COBISS.SR-ID 224210956
