CENTAR ZA EVROATLANTSKE STUDIJE - CEAS

napredak, posvećenost, uticaj

14 TAČAKA OMBUDSMANA I POVERENIKA ZA INFORMACIJE OD JAVNOG ZNAČAJA I ZAŠTITU PODATAKA O LIČNOSTI

***

AKCIONI PLAN JAVNOG ZAGOVARANJA USVAJANJA PREDLOGA

ANALIZA CENTRA ZA EVROATLANTSKE STUDIJE

MART 2014

Analiza je deo projekta „Promocija sveobuhvatne reforme sektora bezbednosti" koji je podržala Nacionalna zadužbina za demokratiju iz Vašingtona

National Endowment for Democracy
Supporting freedom around the world

*"**N**e treba čekati na zakon i ne raditi ništa. Ne treba zaboraviti da osim usvajanja zakona postoji još nešto, u najmanju ruku podjednako važno, možda i važnije. Ni najbolje napisan zakon nije dovoljno dobar ako nije obezbeđena njegova dosledna primena. A verovatno najbitnija pretpostavka dosledne, kvalitetne primene jest puna svest o značaju onoga na šta se zakon odnosi."*

Rodoljub Šabić
Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti

Sadržaj

UVOD

Pitanja u vezi sa osnovnim ljudskim pravima, pravom na privatnost i zaštitom podataka kada je reč o elektronskim i drugim komunikacijama, prenosu poruka žičnim i/ili bežičnim putem (fiksna i mobilna telefonija, satelitski tele- linkovi) i njihovom nadzoru postala su tokom 2013. godine pitanja svakodnenvnice. Podaci o nadzoru elektronskih komunikacija koji je (NSA) američka Nacionalna agencija za bezbednost sprovodila širom sveta, a koje je tokom proleća 2013. godine obelodanio Edvard Snouden (Edward Snowden) podstakli su pitanja o zaštiti podataka i prava na privatnost u zemljama Zapadne međunarodne zajednice. NSA je navodno špijunirala lidere Nemačke, Brazila, Meksika, i još najmanje 35 svetskih lidera, zatim sedište Svetske banke, Međunarodnog monetarnog fonda, Ujedinjenih nacija, Evropsku uniju, Evropski parlament, itd.

Kao odgovor na ovaj skandal, američki predsednik Barak Obama (Barack Obama) imenovao je petočlani panel, odnosno petočlanu Revizorsku grupu za obaveštajno-komunikacione tehnologije da preispita praksu američkog nadzora elektronskih komunikacija i sastavljanja masovnih bazi podataka o milijardama telefonskih poziva u, iz, ili ka SAD

U izveštaju koji je objavila Bela kuća krajem decembra 2013. godine, petočlani panel predlaže nove mere zaštite i ograničenja za različite obaveštajne programe, uključujući i preporuku da se skladištenje podataka o pozivima prepusti privatnom sektoru – ili potpuno novom entitetu koji bi prikupio informacije od telefonskih kompanija, ili samim operaterima. Preporuke koje se nalaze u ovom izveštaju biće razmatrane u toku sledeće godine.

Za to vreme u Srbiji, skoro godinu dana pre afere Snouden, u julu 2012. godine, Ombudsman Saša Janković i Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Rodoljub Šabić, ukazali su na alarmantni raskorak između ustavnih prava - kada je reč o praćenju elektronskih komunikacija i zaštiti podataka - i prakse, kao i na probleme koje takva situacija može izazvati i već izaziva, predstavljajući 14 tačaka, odnosno preporuka, kako bi se ovakva situacija prevazišla.

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti uputio je Vladi Srbije, još u oktobru 2012. godine - **Inicijativu za donošenje Zakona o bezbednosnim proverama** ocenjujući da je materija bezbednosnih provera uređena u nekoliko zakona i drugih propisa, ali na neodgovarajući način. Razlog tome je što se vršenje bezbednosnih provera uređuje samo u kontekstu materije koja se neposredno uređuje predmetnim zakonima i drugim propisima. To su po pravilu oni zakoni, odnosno drugi propisi kojima se uređuje materija zapošljavanja u državnim organima, naročito u policiji, vojsci i službama bezbednosti, kao i materija školovanja u školskim ustanovama koje su prohodne za zapošljavanje u navedenim državnim organima.

CEAS je više puta u javnosti ukazivao na problem nepostojanja posebnog Zakona o bezbednosnim proverama, odnosno zagaovarao donošenje posebnog Zakona koji bi regulisao ovu oblast.

CEAS smatra da je u interesu svih građana Srbije, države Srbije i industrije privatnog sektora bezbednosti da se i takve ocene, to jest zaključci koji proizilaze iz bezbednosnih provera fizičkih lica, stave pod demokratsku kontrolu, sa ciljem da se na pouzdan način spreče moguće zloupotrebe. Potrebno je hitno zakonom definisati pojam i procedure termina bezbednosna provera, kako to Ustav Srbije i nalaže. Imajući u vidu ko sve može i treba da vrši spomenute provere, smatramo da je ovo najbolje rešiti posebnim Zakonom o bezbednosnim proverama.

Međutim, tada, kao ni sada, godinu i po dana nakon zvaničnog predstavljanja 14 tačaka, u Srbiji nema dovoljno jake političke volje da se ova oblast uredi. Uprkos brojnim, još uvek nerazjašnjenim skandalima kada je reč o nadzoru elektronskih komunikacija i prisluškivanju koji dopiru i do samog državnog vrha, činjenici da godinu dana nakon afere prisluškivanja predsednika Srbije Tomislava Nikolića i prvog potpredsednika Vlade Aleksandra Vučića, Nikolić tvrdi da ga i dalje prisluškuju, kao i redovnim javnim apelima Ombudsmana i Poverenika, još uvek ne postoji politički konsenzus, a ni politička volja, da se ovakvo stanje konačno prevaziđe zakonskom regulacijom oblasti praćenja i pristupa elektronskim komunikacijama.

CILJ I METODOLOGIJA AKCIONOG PLANA

U okviru projekta "*Promocija sveobuhvatne reforme sektora bezbednosti*" koji je podržala Nacionalna zadužbina za demokratiju iz Vašingtona, SAD, Centar za evroatlantske studije je, nakon iscrpnih konsultacija sa Zaštitnikom građana (Ombudsmanom), Sašom Jankovićem, Poverenikom za informacije od javnog značaja i zaštitu podataka o ličnosti (Poverenikom), Rodoljubom Šabićem, i službenicima njihovih Kancelarija, sproveo detaljnu analizu predloženih 14 tačaka povodom zaštite prava na privatnost i povezanih ljudskih prava. Ovaj Akcioni plan rezultat je spomenute analize.

OPŠTI POLITIČKI I BEZBEDNOSNI KONTEKST

U julu 2012. godine, Ombudsman i Poverenik su ukazali na alarmantni raskorak između ustavnih prava - kada je reč o praćenju elektronskih komunikacija i zaštiti podataka - i prakse, predstavljajući 14 tačaka, odnosno preporuka, kako bi se ovakva situacija prevazišla. Preporučeni koraci bili su sledeći:

1. Vlada bi trebalo da pravi nacrte i predlaže, a Skupština da usvaja, samo takve zakone koji poštuju ustavne garancije koje se tiču privatnosti komunikacija i drugih ljudskih prava. Mišljenje državnih organa uspostavljenih da štite prava građana Narodna skupština ne bi trebala da ignoriše.
2. Hitno izmeniti relevantne zakone kako bi se odredilo koji konkretni sudovi imaju nadležnost da odlučuju o zahtevima policije, Vojnobezbednosne agencije (VBA) i Vojnoobaveštajne agencije (VOA) da pristupe podacima o komunikacijama građana (po postojećim propisima nadležnost suda poznata je samo za Bezbednosno-informativnu agenciju - BIA i MUP).
3. Primeniti efikasne organizacione mere i IT rešenja koje ubrzavaju prethodnu sudsku kontrolu i odlučivanje o zahtevima za pristup komunikacijama i podacima o komunikacijama.
4. Ujediniti postojeće paralelne tehničke mogućnosti različitih agencija i policije u jednu, nacionalnu agenciju koja, kao provajder, pruža tehničke usluge neophodne za presretanje komunikacija i drugih signala svim autorizovanim korisnicima.
5. Ujediniti procedure prema pružaocima elektronskih komunikacija i njihove obaveze.
6. Obezbediti neizbrisivo beleženje pristupa telekomunikacijama, uz sve podatke koji su potrebni da bi se mogla izvršiti naknadna kontrola zakonitosti i pravilnosti pristupa.
7. Nastaviti sa pravnim uređenjem rada privatnog sektora bezbednosti. Rok za usaglašavanje podzakonskih opštih akata vezanih za Zakone o privatnom obezbeđenju i detektivskoj delatnosti donete 06.12.2013. godine je 06.05.2014. godina
8. Omogućiti jaku, pravnu i faktičku zaštitu uzbunjivača (posebno u sektoru bezbednosti, ali i uopšte) i poveriti zaštitu Zaštitniku građana.

9. Kriminalizovati ometanje istrage koju vode nezavisni kontrolni državni organi (Zaštitnik građana, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Agencija za borbu protiv korupcije, Državna revizorska institucija, Poverenik za zaštitu ravnopravnosti). Bilo koje uznemiravanje, pretnja ili drugi pokušaj da se utiče na pritužioca ili svedoka koji sarađuje sa kontrolnim organima trebalo bi inkriminisati kao posebno krivično delo "ometanje istrage" kada je reč o navedenim subjektima.
10. Obavezati unutrašnje nadzorne mehanizme da o svojim nalazima od značaja za poštovanje ljudskih prava obaveštavaju Zaštitnika građana i nadležne skupštinske odbore, posebno u slučajevima kada se o njih oglušilo rukovodstvo organa u kojima su obrazovani i u slučajevima koji govore o ozbiljnim navodnim ili potvrđenim kršenjima ljudskih prava.
11. Preispitati rezultate sprovođenja Zakona o tajnosti podataka (uključujući usvajanje neophodnih poduzakonskih akata, deklasifikaciju starih dokumenata, sprovođenje istraga, izdavanje bezbednosnih sertifikata...) i preduzeti ozbiljne izmene tog zakona ili donošenje novog.
12. Jačati kapacitet nadzornih institucija da rukuju sa poverljivim podacima i čuvaju ih.
13. Usvojiti novi Zakon o Bezbednosno-informativnoj agenciji kako bi se, između ostalog, obezbedila predvidljivost u upotrebi posebnih mera.
14. Razmotriti policijska ovlašćenja obaveštajno/bezbednosnih službi, odnosno njihovo učešće u krivičnim postupcima.

U Srbiji imamo problematičnu situacijikoja otvara mogućnost nekontrolisanom pristupu ličnim podacima kao i komunikaciji građana, i koja je ostala je neprimećena sve do novembra 2012. godine, odnosno dok nije lično dotakla predsednika Srbije, Tomislava Nikolića, i (tadašnjeg) ministra odbrane, koordinatora rada svih službi bezbednosti i prvog potpredsednika Vlade Srbije, Aleksandra Vučića. Gostujući u emisiji Svedok na RTS-u, predsednik Srbije Tomislav Nikolić izjavio je: „Mi smo tu upali u *zmijsko gnezdo*, među ljude koji koriste visoke funkcije u mnogim službama da gospodare životima, među ljude koji su se drznuli da prisluškuju najpre mene, pa onda i Aleksandra Vučića. To će morati da se istraži do kraja. Tako u Srbiji ne može da se živi". Ova vest sutradan je odjeknula u svim medijima, uz izjave Aleksandra Vučića, koji je potvrdio Nikolićevu tvrdnju od prethodnog dana, najavljujući opsežnu istragu i promene. Informacije o mreži prisluškivanja Vučić je dobio od Bezbednosno-informativne agencije (BIA), koja ga je obavestila da je tri dana ranije deo Ministarstva unutrašnjih poslova izdao nalog za praćenje njegovog i Nikolićevog telefona, navodno, kako je rekao: "jedne grupe po nalogu MUP-a".

Centar za evroatlantske studije je povodom ove afere reagovao saopštenjem za javnost, pozivajući sve iskrene proevropske snage u Srbiji da zahtevaju što hitnije usvajanje potrebnih zakona i drugih akata koji bi doveli do njihove primene i da ne dopuste da se zbog drugih prioriteta - dijaloga Beograda s Prištinom - aktuelnim vlastima u Srbiji progleda kroz prste za sve očitiju nesposobnost ili odsustvo namere da održe prethodno postignuti nivo demokratskih procedura i podele vlasti, a kamoli da ih unapređuju.

Nedavne afere prisluškivanja predsednika nisu jedini primer delovanja otuđenih centara moći. Pre izvesnog vremena došlo se do otkrića da je na 16 kontrolisanih objekata RHMZ pronađeno vise od 430 antenskih uređaja nejasnog porekla. Ni povodom toga ništa nije nije preduzeto, stoga CEAS insistira na sistemskim rešenjima razotkrivanja i onemogućavanja delovanja otuđenih centara moći – bez obzira koje su ličnosti potencijalne "žrtve" upotrebe ili zloupotrebe ovlašćenja.

CEAS je takođe konstatovao da se medijsko-stručna rasprava o činjenici, kako je to ministar Dačić rekao: "da je uprava kriminalističke policije tražila listinge ne znajući, kako oni kažu, da je u pitanju telefon Aleksandra Vučića", fokusirala, nažalost, više na to ko za koga radi i zašto baš sada, nego na suštinu problema – protivustavnost dela i odsustvo demokratskog nadzora nad sektorom bezbednosti. I jedan i drugi uzrok pogoduju opasnom trendu uspostavljanja partijskih kontrola nad delovima aparata, čime se uveliko otežava i njegov profesionalni rad. Baš je zato bitno, kako se to, doduše veoma tiho, moglo čuti tih dana, a od strane pojedinih državnih zvaničnika – učiniti javnim sadržaj mera za kontraobaveštajnu zaštitu najviših državnih funkcionera. Navodi da je deo MUP-a delovao protivustavno potpuno su, nažalost, marginalizovali i sami objekti praćenja, Vučić i Nikolić. Za razliku od njih, Ombudsman i Poverenik nastavili su da ukazuju na srž problema. Predlog u četrnaest tačaka, koji za cilj ima poboljšanje situacije u sektoru bezbednosti, morao bi dobiti objedinjenu podršku svih iskrenih demokratskih i proevropskih snaga u srpskom društvu.

Međutim, više od godinu dana nakon ove afere, Predsednik Srbije Tomislav Nikolić tvrdi da afera „prisluškivanje„ još uvek nije okončana i da njega i dalje tajno prisluškuju, ističući da postoji deo Ministarstva unutrašnjih poslova koji ne radi svoj posao kako treba i da postoje ljudi koji sabotiraju njegovu bezbednost. Predsednik Srbije ilustrovao je situaciju izjavom da je, kada ga je pozvao predsednik Vlade i rekao mu da u okviru akcije „Grom" MUP *kreće u veliku akciju*, on rekao da prekine jer ih „možda neko prisluškuje". Ono što je zanimljivo je – ko bi to mogao da ih prisluškuje? Ako je neka službena Agencija, ili ponovo uprava kriminalističke policije, kako ih Dačić targetirao krajem 2012 godine, zar oni ne bi trebali da znaju za akciju Grom? Ako i ne znaju – zar ne bi, prema svojim ovlašćenjima i delokrugu rada, trebalo da znaju? Ukoliko ih pak ne prisluškuju službeni organi, znači li to da to čine kriminalci?

Prema tome, uprkos pozitivnim koracima kao što je činjenica da Vojno-bezbednosna agencija (VBA) i Bezbednosno-informativna agencija (BIA) više bez odluke suda ne zadiru u privatnost komunikacije, i dalje postoje zabrinjavajući problemi kada je u pitanju pravo na privatnost i zaštitu podataka građana Srbije. Policija i dalje prisluškuje građane pozivajući se na Zakon o krivičnom postupku. Kod operatora koji broji pristupe elektronskim komunikacijama građana Poverenik je tokom 2012. godine utvrdio da je BIA imala skoro duplo manji broj upita od Vojnobezbednosne agencije, dok je MUP Srbije imao hiljadu puta više od vojne, i dve hiljade puta više od civilne službe bezbednosti.

Prema ocenama Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka Vlade R. Srbije od stupanja na snagu Zakona o tajnosti podataka, januara 2010. godine, do danas, najznačajnije probleme, sa aspekta rada Kancelarije, predstavljaju nepoznavanje Zakona od strane organa javne vlasti, kao i neusklađenost normative, posebno ako se ima u

vidu da su pojedina zakonska i podzakonska akta doneta nakon januara 2010. godine koristila termin službena tajna i vojna tajna, iako su ovi termini ukinuti Zakonom, kao i da se na neadekvatan način postupalo sa tajnim podacima.

Prema rečima Ombudsmana Saše Jankovića, samo jedan operater u Srbiji zabeležio je za godinu dana preko 4.000 pristupa po zahtevu i preko 270.000 pristupa neposredno. Telefonskih operatera u Srbiji ima četiri, te ukupna cifra pristupa komunikacijama građana po nekim procenama dostiže oko milion godišnje. Tačnog broja nema jer ostali operateri nisu brojali pristupe podacima o komunikacijama svojih korisnika, niti uskratili pristup kada za njega nema zakonom propisanih uslova.

Tu je takođe i pitanje bezbednosnih provera koje su zakonom propisane ali ne i definisane u smislu koji se podaci prikupljaju u koje svrhe, kako se čuvaju, kome su dostupne i da li je zabranjeno da se koriste u druge svrhe i sl. Naime, Poverenik je pre više od godinu dana uputio inicjativu Vladi Srbije da predloži poseban zakon o bezbednosnim proverama (Inicijativa je priložena u Aneksu ovog dokumenta). Zakon bi definisao pojam bezbednosne provere i procedure koje iz nje proističu, kako to Ustav Republike Srbije i zahteva. Ministar policije Ivica Dačić najavio je da je ovo pitanje otvoreno i da se mora precizirati izmenama i dopunama Zakona o policiji. Ovo pitanje je trenutno regulisano samo Zakonom o evidencijama koji je usvojen 1996. godine pa se samim tim ne može smatrati aktuelnim u pogledu razvoja tehnologije, niti pruža jasnu definiciju koji se podaci prikupljaju i za koje potrebe.

U Srbiji se, dakle, u pojedinim delovima sektora bezbednosti, zadiranje u lične podatke i komunikaciju građana još uvek smatra bespogovornim pravom bezbednosnih službi i policije. Činjenica je da je to pitanje, dok ga Poverenik i Ombudsman nisu otvorili, bilo u zoni „ne pitaj, ne pričaj“. I kako je Ombudsman rekao: “Čak je u jednom momentu i Narodna skupština branila „pravo“ službi da po sopstvenom nahođenju pristupaju tim podacima, bez odluke bilo koga drugog, a kamoli suda - kako zahteva Ustav. “

Kao što postoje dve vrste evidencija – MUP I BIA, sa dosijeima i potencijalnim prekršiocima, tako postoje i dve vrste preliminarnih istraga – krivična i ugrožavanje ustavnog poretka. Osnovno pitanje je kada i prema kome počinje preliminarna istraga – odnosno - koje su to dozvoljene forme i metode rada javnih i tajnih službi bezbednosti. Odgovor možda leži u izvoru njihovog finansiranja. (*samo budžet ili postoji alternativni fond?*)

Dodatni problem je činjenica da građani Srbije, uprkos relativnom poverenju koje imaju u nezavisne institucije, smatraju da Ombudsman i Poverenik nemaju dovoljno uticaja na odluke Vlade. Istraživanje javnog mnjenja koje je Centar za evroatlantske studije sproveo tokom aprila i maja meseca 2013. godine ukazao je na problem veoma podeljenih stavova prema nezavisnim institucijama generalno, ali i prema instituciji Ombudsmana i Poverenika konkretno.

Tako je 37% građana ocenilo da ima poverenja u nezavisne institucije, 31% građana nema poverenja u iste, dok 32% građana Srbije nema stav o ovom pitanju. Kada se rezultati pogledaju bliže, Zaštitnik građana u očima građana Srbija ima slab ili nikakav uticaj na odluke Vlade – 2% građana smatra da ima jak uticaj, 10% umeren, 33% slab, 28% građana smatra da ga nema, dok 27% građana nema stav. Situacije je slična i kada je u pitanju Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, za koga 3%

građana smatra da ima jak uticaj, 11% umeren, 32% slab, 29% građana smatra da ga nema, a 25% građana nema stav.

Situacija se, dakle, ni godinu i po dana nakon što su Ombudsman i Poverenik predstavili svoj predlog u 14 tačaka, nije značajno promenila. Nacrt izmenjenog zakona o elektronskim komunikacijama, prema rečima Poverenika, još uvek rizikuje da sadrži određene formulacije koje bi mogle da izazovu dileme u pristupu podacima o komunikaciji građana.

Poverenik je, takođe, još jednom insistirao na potrebi da se utvrdi obaveza operatera o vođenju evidencija o broju pristupa podacima, što predstavlja ponovni poziv na ujedinjenje procedura prema pružaocima usluga elektronskih komunikacija i njihove obaveze (*tačka 5*).

Čak se ni uvođenjem „dvostrukog ključa" u Bezbednosno-informativnoj agenciji nisu prevazišli neki od postojećih problema. U izveštaju evropskog eksperta Mauricija Varanezea (Maurizio Varanese) o proceni rada službi bezbednosti u Srbiji iz marta ove godine navodi se da BIA zapravo funkcioniše kao „provajder" za sve druge službe, odnosno da „uvek kada policija ili VBA žele da izvrše presretanje komunikacije u svrhe istrage, sudski nalog se uručuje BIA ili VBA, koji preko tehničke opreme koju poseduju dupliraju i usmeravaju telefonsku liniju prema Službi za specijalne istražne metode (SSIM) u Upravi kriminalističke policije, koja od pre nekog vremena vrši stvarno presretanje telefonskih razgovora vlastitom opremom ili preusmeravanjem sa opreme operatera".

Kao poslednji element ovakvog alarmantnog stanja navodi se i činjenica da je Zakon o slobodnom pristupu informacijama zapravo jedini zakon koji uglavnom krše samo funkcioneri, jer ne postoji mogućnost da ga prekrše obični građani. Međutim, prema rečima Poverenika, u poslednje vreme, uprkos ovoj činjenici, nije pokrenut nijedan postupak protiv prekršioca, dok Poverenik još uvek nema pravo da pokrene prekršajne postupke.

Naprotiv, prema njegovom zaključku, u odsustvu strateškog, osmišljenog pristupa pitanjima zaštite podataka o ličnosti, Vlada Srbije nekim svojim aktivnostima i inače brojnim postojećim problemima u ovoj oblasti dodaje i nove. Pripremaju se i predlažu zakoni i podzakonski akti u kojima se obrada podataka o ličnosti tretira na način koji nije u skladu sa Ustavom i Zakonom o zaštiti podataka o ličnosti. (Npr. Predlog zakona o izvozu i uvozu robe dvostruke namene).

Obzirom da prilikom eksplanatornog skrininga za poglavlja 23 i 24 nije bilo reči o radu policije i pravosuđa kada je u pitanju jedinstvena kontrola nad prisluškivanjem (monitoring sistem), osim napomene da je potrebno bolje urediti oblast zaštite podataka o ličnosti i uprkos činjenici da su i nezavisne institucije dale svoje mišljenje prilikom prezentacija u Briselu, bliže otvaranje ove oblasti očekuje se po dolasku stručnjaka iz EU koji tek treba da procene situaciju.

REALIZOVANE PREPORUKE

Izmenom Zakona o VBA i VOA, u februaru 2013. godine, Ustavni sud proglasio je neustavnim određene članove predmetnih Zakona, čime je utvrđeno da direktor Vojnobezbednosne agencije (VBA) može da daje nalog za tajni elektronski nadzor komunikacija samo uz odobrenje suda i da viši sud na području apelacionog suda na kome se preduzma mera odobrava tajni elektronski nadzor telekomunikacija, čime se može ostvariti uvid u "listing" (Član 12, stav 1, tačka 6 Zakona: *Tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju, bez uvida u njihov sadržaj*). Usvojen je i amandman ombudsmana Saše Jankovića čime je utvrđeno da ako VBA ili VOA dođu u posed podataka i informacija iz nadležnosti drugih službi bezbednosti ili policije, te podatke i informacije dostaviće drugim službama bezbednosti ako su od značaja za nacionalnu bezbednost, a policiji ako se odnose na krivična dela na koja se, u skladu sa odredbama Zakonika o krivičnom postupku, primenjuju posebne dokazne radnje.

Drugi pomak načinjen je u julu 2012. godine uvođenjem sistema „duplog ključa" u Bezbednosno-informativnoj agenciji (BIA) prilikom presretanja komunikacije. „Dvostruki ključ" onemogućava da se samo sa jednog mesta aktivira prisluškivanje bilo čijeg telefonskog broja, čime će mogućnost zloupotrebe elektronskog nadzora komunikacija građana biti svedena na još manju meru.

Nadalje, septembra 2013 godine donet je niz Uredbi koje bliže uređuju Zakon o tajnosti podataka, kao što su Uredba o bližim kriterijumima za određivanje stepena tajnosti "državna tajna" i "strogo poverljivo" *("Sl.Gl. RS", br. 46/2013* od 24.5.2013. godine, koja je stupila na snagu 1.6.2013, a primenjuje se od 1.9.2013.), Uredba o bližim kriterijumima za određivanje stepena tajnosti "poverljivo" i "interno" u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka *("Sl.Gl. RS", br. 86/2013* od 30.9.2013. godine, koja je stupila na snagu 8.10.2013.), i Uredba o bližim kriterijumima za određivanje stepena tajnosti "poverljivo" i "interno" u Bezbednosno-informativnoj *agenciji ("Sl.Gl. RS", br. 70/2013* od 7.8.2013. godine, koja je stupila na snagu 15.8.2013, a primenjuje se od 1.9.2013.), kojima se jača kapacitet Zakona kako je to preporučeno tačkom 11.

U postupku je i donošenje Uredbe o bližim kriterijumima za određivanje dokumentata stepena tajnosti „poverljivo" i „interno" za najveći broj organa javne vlasti, kao i Zakona o tzv. Informacionoj bezbednosti koji bi normativno trebalo da zaokruži oblast zaštite tajnih podataka na nacionalnom nivou.

Iz Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka ukazuju i na to da je u toku formiranje Radne grupe za izmene i dopune Zakona o tajnosti podataka, koja ima za cilj otklanjanje uočenih manjkavosti i pravnih praznina postojećeg Zakona, kao i stvaranje uslova za efikasniju primenu samog Zakona.

U decembru 2013 godine donet je Zakon o privatnom obezbeđenju i Zakon o detektivima, čime je započeto normativno uređenje privatnog sektora bezbednosti. Komisija za JP partnerstvo u sektoru bezbednosti republike Srbije, čiji je CEAS je član, u saradnji sa MUP Srbije predstavila je na okruglom stolu održanom u februaru 2014 godine, nacrte 3 Pravilnika koje detaljno regilišu program i uslove sprovođenja obuke izvršioca privatnog

obezbeđenja i postupak izdavanja licence, bez kojih ovaj Zakon nije primenjiv. Rok za donošenje ovih Pravilnika je 06.05.2014. godina, i ukoliko do tada bude sastavljenja Vlada R Srbije, odnosno imenovan nadležni ministar – čiji se potpis za stupanje na snagu ovih Pravilnika čeka – one će biti na snazi u propisanom roku. Pored toga, spremno je još 4 Pravilnika i 2 Uredbe, koje će se u narednom periodu predstaviti zainteresovanim licima i ući u postupak donošenja.

PRIMERI DOBRE PRAKSE I DRUGE INICIJATIVE

Ujedinjeno Kraljevstvo

Kancelarija Poverenika za informacije je nezavisna agencija koja vodi javni registar kontrolora podataka i sprovodi Zakon o zaštiti podataka, propise koji se odnose na privatnost i elektronske komunikacije i Zakon o slobodi informisanja.

Kancelariji je mandat proširen 2010. godine u vidu povišenog mogućeg iznosa za izrečene kazne na £500,000 za ozbiljna kršenja principa zaštite podataka, jačajući njene relativno ograničene izvršne moći. Kancelarija je izdala smernice o okolnostima pod kojima se nova ovlašćenja za izricanje kazni koriste. Prema njima, Kancelarija mora da utvrdi da je došlo do ozbiljnog kršenja prava, odnosno da postoji velika mogućnost izazivanja značajne štete ili patnje osobe na koju se podaci odnose, kao i da li je kršenje bilo namerno ili ne.

Takođe, Kancelariji su date nova ovlašćenja u smislu mogućnosti revizije u državnim organima bez njihovog pristanka. Napisan je i Kodeks prakse koji definiše nova revizorska ovlašćenja.

Presretanje komunikacije regulisano je Uredbom o istražnim ovlašćenjima (Regulation of Investigatory Powers Act 2000 - RIPA). Uredba daje ovlašćenje ministru unutrašnjih poslova da izdaje naloge za presretanje komunikacije i zahteva od pružaoca telekomunikacionih usluga da obezbede razumnu mogućnost presretanja na svojim mrežama. Uredba takođe daje mogućnost da bilo koji državni organ, ovlašćen od strane ministra unutrašnjih poslova, pristupi podacima o komunikaciji bez naloga. Ovi podaci odnose se na izvor, odredište i tip bilo koje komunikacije, kao što su informacije o lokaciji mobilnog telefona lokaciju i parcijalni logovi internet pretraživača, dok se, na primer, kompletan URL smatra sadržajem za koji je neophodan nalog.

Zahteve za presretanje i podatke o komunikacijama pregleda Poverenik za presretanje komunikacija, bivši sudija Višeg suda.

Jedan od najradikalnijih koraka u pogledu regulisanja zaštite podataka, britanska Vlada načinila je 2011. godine, centralizovanjem bezbednosnih podataka. Naime, bezbednosnu proveru za lica za koja je, po osnovu drugih propisa, potrebna predhodna bezbednosna provera, za Tajnu obaveštajnu službu (Secret Intelligence Service - MI6), Službu bezbednosti (Security Service - MI5) i Štab Vlade za komunikacije (Government Communications Headquarters - GCHQ) sada obavlja jedno nezavisno telo – 2011 godine Agencija za bezbednosne provere postala je Služba za bezbednosne poslove – Nacionalne

bezbednosne provere, koja se sada sa svojim FCO kolegom (služba FCO) kao jedini provajder NSV-a za celu vladu.

Holandija

Holandska agencija za zaštitu podataka, College Bescherming Persoonsgegevens – CBP, nadgleda da li je rukovanje evidencijama ličnih podataka u skladu sa Zakonom o zaštiti ličnih podataka. Iako su ovlašćenja agencije mahom ostala ista još od njenog osnivanja, njene izvršne moću su relativno porasle u vidu mogućnosti korišćenja administrativnih mera i izricanja kazni za nepoštovanje. Agencija takođe može i da naplati novčane kazne do EUR 4,500, za kršenje zahteva o obaveštenju koji propisuje član 75 Zakona o zaštiti ličnih podataka (Dutch Personal Data Protection Act - PDPA). CBP je istovremeno i savetodavno telo holandske Vlade, bavi se pritužbama koje podnesu osobe na koje se prikupljeni podaci odnose, pokreće istrage i daje preporuke kontrolorima ličnih podataka.

U januaru 2008. godine, predsednik CBPa pozvao je na povećanje nadzorne moći njegove institucije kako bi se ujedno ojačalo i sprovođenje Zakona o zaštiti podataka i preduzele direktne mere koje se tiču istraga i kazni.

Presretanje komunikacije u Holandiji, što konkretno znači skeniranje i arhiviranje sadržaja komunikacije, regulisano je Krivičnim zakonikom i zahteva sudski nalog (član 125. Zakona o krivičnom postupku). Obaveštajnim službama sudski nalog nije potreban za presretanje, ali moraju imati ovlašćenje ministra unutrašnjih poslova.

Zakon o posebim ovlašćenjima u istragama dalje unapređuje istražne metode. Zakon o telekomunikacijama zahteva da svi pružaoci telekomunikacionih usluga imaju kapacitet za presretanje telefonskih i internet komunikacija, ali da ovakve usluge pruže samo uz sudski nalog. Posebna agencija, Agencija za radio-komunikacije Holandije, odgovorna je za sprovođenje postupaka prisluškivanja u sektoru za telekomunikacije.

Zakon o obaveštajnim i bezbednosnim službama omogućava i presretanje, pretragu i skeniranje satelitske komunikacije. Takođe dozvoljava obaveštajnim službama da čuvaju podatke o presretnutim komunikacijama do godinu dana. Čuvanje šifrovanih podataka nije vremenski ograničeno. Nacionalna SIGNIT organizacija (NSO) osnovana je 2003. godine od strane holandskih obaveštajnih službi za presretanje svih satelitskih komunikacija.

Švedska

Švedski Zakon o ličnim podacima unosi zahteve Evropske unije o zaštiti podataka usvojene Direktivom 1995/46/EC u nacionalni zakonodavni okvir. Zakon reguliše uspostavljanje i upotrebu automatskih evidencija koja se odnose na fizička lica, kako u javnom, tako i u državnom sektoru.

Poštovanje Zakona o ličnim podacima prati Odbor za pregled podataka (Data Inspection Board - DIB), nezavisna državna agencija. Zakon o ličnim podacima zahteva da se Odbor obavesti o svakoj automatskoj obradi podataka. Osim nekoliko izuzetaka koji se odnose na obavezu obaveštenja, obrada podataka koja nosi veliki rizik nepropisnog zadiranja u privatnost zahteva obaveštavanje Odbora za pregled podataka, kako bi se sprovela preliminarna provera. Međutim, ovlašćenja DIB - a se mogu videti kao relativno ograničena, jer Odbor može da daje preporuke, ali sprovođenje istih zavisi od odluke suda.

Švedska Vlada je 2004. godine uspostavila Odbor za zaštitu privatnosti, sastavljen od relevantnih stručnjaka i narodnih poslanika, sa mandatom da analiziraju postojeće zakone koji se tiču privatnosti i sprovedu anketu u vezi sa ovim pitanjem. Zbog kritika da je Zakon o ličnim podacima previše restriktivan, švedski Parlament je 2006. godine izglasao je amandmane kako bi zakon postao više usmeren na sprečavanje zloupotrebe ličnih podataka.

Odbor je jasno identifikovao i nedostatak institucije koja bi nosila krovnu odgovornost za pitanja povezana sa problemom privatnosti i predložila da se ta dužnost poveri potpuno novoj agenciji, ili da se barem Odboru za pregled podataka daju šira ovlašćenja. Ovo je rezultiralo uspostavljanje Komisije za bezbednost i zaštitu integriteta (Commission on Security and Integrity Protection - SÄKINT), nezavisno telo koje bira parlament - zaduženu za praćenje i kontrolu nad upotrebom tajnog nadzora od strane policije i tajnih službi.

Svaka upotreba video zapisa, kao i nadzora i prisluškivanja komunikacija, zahteva sudski nalog u skladu sa Zakonom o merama za istragu ozbiljih zločina i Zakona o sudskom postupku. Zakoni o video i audio nadzoru vremenom su se razvili i delom postali elementi Zakona o sudskom postupku, paralelno sa novim zakonima koji regulisanjem ove dve oblasti daju velika ovlašćenja tajnim službama. Kada je 2006. godine predložen zakon koji je trebalo da proširi još više upotrebu tajnog nadzora, uključujući, između ostalog, zakon kojim je previđeno prisluškivanje telefonskih razgovora iz preventivnih razloga, Parlament je odlučio da raspravu o zakonu odloži dok se u njega ne unesu i uredbe o merama zaštite od zloupotrebe, uključujući obavezu policije da obavesti osobe koje su subjekti tajnog nadzora, kada god se to smatra da je bezbedno iz istražnih razloga.

Još jedan kontroverzni zakon usvojen je 2008. godine, dozvoljavajući Radio ustanovi Nacionalne Odbrane (Försvarets Radioanstalt - FRA) da koristi poseban softver za pretragu osetljivih ključnih reči u svim telefonskim i e-mail komunikacijama koje prolaze kroz kablove ili žice preko granica zemlje, bez sudskog naloga. Kako je zakon predstavljao pretnju preko-graničnoj komunikaciji, odnosno, omogućavao praćenje elektronske komunikacije osoba koje se ne nalaze u okviru granica Švedske, nakon brojnih kritika javnosti i grupa koje se bave pitanjem privatnosti, Zakon je izmenjen.

Slovenija

U Sloveniji je pravo na privatnost zagarantovano Ustavom, kao i Zakonom o zaštiti ličnih podataka. Zakon o zaštiti podataka redovno se ažurira usled razvoja tehnoloških dostignuća, poput video-nadzora, biometrijskih podataka, i sl. i u skladu je sa Direktivom o zaštiti podataka EU.

Dalje, član 150 Krivičnog zakonika zabranjuje neovlašćeno otvaranje pisama i drugih poštanskih poruka i presretanje poruka koje se prenose preko telekomunikacionih mreža. Takođe, zabranjeno je i neovlašćen pristup sadržaju poruka koje se prenose putem telefona ili drugih telekomunikacionih tehnologija , kao i neovlašćeno prosleđivanje pisama na treće lice. Član 151 Zakona dalje zabranjuje i objavljivanje privatnih komunikacija bez saglasnosti od strane ovlašćenog lica.

Zakon o zaštiti ličnih podataka takođe određuje da je sve što nije izričito dozvoljeno u vezi sa prikupljanjem i obradom ličnih podataka zabranjeno. Državna tela mogu da obrađuju lične podatke samo u srvhu za koju imaju zakonsko ovlašćenje, dok privatna lica moraju da poseduju i pisanu saglasnost pojedinca. Osobe čiji se lični podaci prikupljaju moraju unapred da budu obaveštene o ovom postupku. Generalno, lični podaci se mogu prikupljati i čuvati samo onoliko dugo koliko je potrebno da bi se ostvario određeni cilj, i moraju biti izbrisani ili blokirani čim je taj cilj ostvaren. Svi izuzeci moraju da budu jasno definisani zakonom.

Spajanjem Kancelarije Inspektorata za zaštitu ličnih podataka i Poverenika za pristup javnim informacijama, Zakonom o Povereniku za informacije, oformljena je Kancelarija Poverenika za informacije, kao autonomna i nezavisna agencija.

Privatnost komunikacije može biti narušena samo uz sudski nalog, kao i ukoliko se takvo narušavanje smatra neophodnim za svrhu krivične istrage ili radi državne bezbednosti. Ova oblast je u Sloveniji regulisana Zakonom o krivičnom postupku i Zakonom o obaveštajno-bezbednosnoj agenciji Slovenije - SISAA, a sprovodi ga policija i obaveštajno-bezbednosna agencija Slovenije – SOVA.

Sudski nalog se mora obezbediti pre kućnog pretresa ili prisluškivanja telefona. Zakon o policiji dozvoljava tajno posmatranje i praćenje, kao i tajnu policijsku saradnju, ali samo u veoma posebnim okolnostima, i uz odobrenje generalnog direktora policije.

Evropska unija

Osnovna prava su u Evropskoj uniji zaštićena pravnim okvirom koji se sastoji od tri komplementarna elementa:

- Generalnim principima i ustavnom tradicijom zajedničkom za sve zemlje članice;
- Poveljom o osnovnim pravima Evropske unije;
- Evropskom konvencijom o ljudskim pravima.

Povelja eksplicitno izdvaja kao posebno pravo zaštitu ličnih podataka i pravo na privatnost.

Lisabonski sporazum stvorio je osnovu za dalji razvoj regulative koja se odnosi na zaštitu podataka, primenljivu na svaku vrstu obrade ličnih podataka, kako u privatnom, tako i u javnom sektoru, uključujući tu i obradu ličnih podataka u procesu saradnje policije i pravosuđa.

Direktiva EU o zaštiti podataka definiše osnove zaštite ličnih podataka koje zemlje članice moraju da usvoje u nacionalnim zakonima i primenjuje se na svaku automatsku obradu i bilo kakvo drugo rukovanje ličnih podataka koje čini deo procesa stvaranja evidencije. Lični podaci definisani su kao svaka informacija koja se odnosi na fizičko lice. Za obradu ličnih podataka zadužen je kontrolor podataka koji obezbeđuje poštovanje principa koji se odnose na kvalitet podataka, ima obavezu da obavesti osobu na koju se podaci odnose o njihovom prikupljanju i ima ovlašćenje da sprovede odgovarajuće tehničke i organizacione mere protiv nezakonitog uništavanja, slučajnog gubitka ili neovlašćenog menjanja, otkrivanja ili pristupanja podacima.

Direktiva takođe zahteva od zemalja članica da obezbede nadzor sprovođenja uredbi kroz nezavisne nadzorne mehanizme. Nadzorni mehanizmi moraju imati istražna ovlašćenja i efektivne nadležnosti za intervenciju, poput ovlašćenja da narede blokiranje, brisanje i uništavanje podataka, ili uspostavljanje privremene ili trajne zabrane za njihovu obradu.

Direktiva je uspostavila i Radnu grupu za zaštitu lica kao konsultativno telo. Radna grupa sastoji se od predstavnika nadzornih institucija zemalja članica i predstavnika Evropskog nadzornika za zaštitu podataka (European Data Protection Supervisor - EDPS).

Evropski nadzornik za zaštitu podataka

Evropski nadzornik za zaštitu podataka jedna je od ključnih institucija u oblasti privatnosti i zaštite podataka u EU. Odgovorna je za nadzor obrade ličnih podataka od strane administracije EU i ima savetodavnu ulogu u pitanjima zakona koji se tiču, ili imaju uticaj na, pravo na privatnost i pravo na zaštitu ličnih podataka, kao i saradnju sa sličnim institucijama.

Radna grupa člana 29

Radna grupa člana 29 (Article 29 Working Party – WP29) služi kao platforma za razmenu i koordinaciju između nadzornih tela zemalja članica EU i kao konsultativno telo. Glavna uloga Radne grupe je da analizira sva pitanja koja se tiču primene nacionalnih mera usvojenih u skladu sa Zakonom o zaštiti podataka EU, kako bi se uspostavila jednobrazna primena; savetuje Evropsku komisiju o stepenu zaštite u Uniji i trećim zemljama; savetuje Evropsku komisiju o merama za očuvanje prava i slobode osoba u smislu obrade ličnih

podataka i svake druge predložene mere koja bi imala uticaj na ta prava i slobode; pruži mišljenje o kodeksu postupanja na nivou EU.

Radna grupa može, na sopstvenu inicijativu, da da preporuke o svim pitanjima koja se tiču privatnosti i zaštite podataka u EU. Do sada je, između ostalog, izdala mišljenje o pitanjima poput biometrijskih podataka u pasošima i vizama, zaštiti ličnih podataka dece, standardnim ugovorima o transferu ličnih podataka koji se obrađuju u trećim zemljama, itd. Mišljenja Radne grupe su zajednička referentna tačka za tumačenje Zakona o zaštiti podataka EU.

Inicijativa Globalna mreža (Global Network Initiative)

Inicijativa Globalna mreža je koalicija IT kompanija, civilnog društva, investitora i akademika. Cilj Inicijative je da obezbedi okvir u kojem pružaoci elektronskih usluga – kompanije – mogu da funkcionišu na principima međunarodnih standarda; obezbedi odgovornost istih kroz nezavisne procene; omogući angažovanje na formiranju politika; i omogući razmenu iskustava među svim zainteresovanim stranama.

Inicijativa je u septembru 2013. pisala vladama zemalja članica Koalicije sloboda na internetu (Freedom Online Coalition) zahtevajući da se uspostavi praksa izveštavanja o zahtevima koje država podnese za nadzor elektronskih komunikacija, kao i da se omogući zakonodavni okvir koji bi dozvolio kompanijama da redovno izveštavaju javnost o zahtevima države koje dobiju od policije i službi bezbednosti.

Dakle iz ovoga proizlazi da većina evropskih zemalja ima sisteme u kojima ne-sudske instance imaju pravo da daju naloge za uvid u dosta široki spektar podataka. Drugo, često se brkaju područja (ne pojmovi) tajnog nadzora i zaštite komunikacija, i zaštite ličnih podataka.

TAČKA 4: UJEDINITI POSTOJEĆE PARALELNE TEHNIČKE MOGUĆNOSTI RAZLIČITIH AGENCIJA I POLICIJE U JEDNU

Ujediniti postojeće paralelne tehničke mogućnosti različitih agencija i policije u jednu, nacionalnu agenciju koja, kao provajder, pruža tehničke usluge neophodne za presretanje komunikacija i drugih signala svim autorizovanim korisnicima

Stavljanje svih paralelnih tehničkih mogućnosti različitih agencija i policije u jednu bi svakako umanjilo mogućnost zloupotreba u presretanju i praćenju telekomunikacija i drugih komunikacija građana u velikoj meri.

Ako uzmemo u obzir kao činjenicu izveštaj jednog od ispitanih 4 operatora mobilne telefonije u Srbiji, u kom stoji da je od 4 400 podnetih zahteva za pristup zadržanim podacima samo dva podnela BIA – možemo zaključiti da BIA ima mogućnost samostalnog pristupa zadržanim podacima, pa samim tim samostalno i bez nadzora njima i raspolaže. Da li MUP ima takvu mogućnost? Da li raspolaganje ovako prikupljenim zadržanim podacima predstavlja zaštitu bezbednosti poretka zemlje i ujedno štiti ustavna prava vlasnika zadržanih podataka, da li to čini iz opravdanih razloga i u skladu sa ustanovljenim ustavnim načelima – su nedoumice zbog kojih je ovaj akcioni plan i nastao. Formiranje jedne nacionalne, nezavisne agencije koja bi kao provajder, pružala tehničke usluge neophodne za presretanje komunikacija i drugih signala svim autorizovanim korisnicima – otklonila bi mogućnost nezakonitog postupanja.

Problem svih vlasti u svetu, a zbog vremenski ograničenih mandata, je strah od centralizacije službi bezbednosti, jer time "seku granu na kojoj sede". To bi se naročito moglo reći za Srbiju, u kojoj dominiraju koalicije i trka za resorima.

Ipak, imajući u vidu situaciju i stanje u sektoru bezbednosti u Srbiji, u kojoj se, prema navodima medija i nekadašnjih funkcionera bezbednosnih službi – poput Momira Stojanovića, bivšeg direktora Vojno-bezbednosne agencije (VBA) – službenici Ministarstva unutrašnjih poslova Srbije (MUP RS) nalaze na platnom spisku tajkuna i narko-dilera, dok se istovremeno na tajnim i nelegalnim platnim spiskovima MUPa nalazi oko dve hiljade ljudi, gde treba naravno uzeti u obzir broj doušnika koji naravno na tajnom platnom spisku postavlja se pitanje izvodljivosti ove tačke. Objedinjavanje paralelnih tehničkih mogućnosti u jednu agenciju može se postaviti kao dugoročni cilj, ali je za njegovo ostvarenje potreban niz kratkoročnih mera.

Prvenstveno, potrebno je izmeniti postojeće zakone. Ombudsman i Poverenik istakli su, u novembru 2012. godine, Zakon o elektronskim komunikacijama, Zakon o Vojnim službama bezbednosti, Zakon o bezbednosno-informativnoj agenciji i Zakon o krivičnom postupku kao najkritičnije.

Zakon o elektronskim komunikacijama

Prvi na listi zakona za koji su Ombudsman i Poverenik istakli da su neophodne promene je Zakon o elektronskim komunikacijama. Ustavni sud Republike Srbije proglasio je neustavnim pojedine odredbe ovog Zakona u pogledu pristupa zadržanim podacima, a koje su bile sporne još prilikom procesa njegovog usvajanja. Ustavni sud je proglasio

neustavnim odredbe članova 128. stav 1., člana 128. Stav 5. i člana 129. stav 4., koje se odnose na pristup zadržanim podacima mimo odluke suda i na ovlašćenje nadležnog ministarstva da bliže uređuje zahteve u vezi sa zadržanim podacima podzakonskim aktom.

Problem je nastao zbog neujednačenog i nekoherentnog pravnog okvira koji se odnosi na zadržane podatke, konkretno na sadržaj komunikacije. Zadržani podaci predstavljaju podatke o komunikaciji koji se ne odnose na sadržinu same komunikacije. Tu se pre svega misli na podatke: o praćenju i utvrđivanju izvora komunikacije, o utvrđivanju odredišta komunikacije, utvrđivanju početka, trajanja i završetka komunikacije, o utvrđivanju vrste komunikacije, o identifikaciji terminalne opreme korisnika, o utvrđivanju lokacije mobilne terminalne opreme korisnika. Na primeru telefonskog razgovora to su podaci: o broju sa kojeg se poziva, o broju na koji se poziva, o datumu i vremenu početka i kraja telefonskog poziva, o trajanju telefonskog poziva, o uređaju koji se koristi u komunikaciji (vrsta mobilnog telefona), kao i podaci o geografskoj lokaciji telefona sa kojeg je izvršen poziv, ali ne i identiteti pozivanih korisnika.

Osporene odredbe su kršile procesne garancije koje poznaje član 41. Ustava Republike Srbije koji predviđa da je odstupanje od nepovredivosti tajnosti pisama i drugih sredstava komuniciranja moguće samo na određeno vreme i na osnovu odluke suda, a ako su neophodna radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom.

Međutim, Nacrt Zakon o izmenama i dopunama zakona o elektronskim komunikacijama preti da ostane neustavan i pored uslovljenosti ograničenja tajnosti komunikacije postojanjem odluke suda. Naime, Poverenik je u završenoj javnoj raspravi o Nacrtu izmena i dopuna Zakona o elektronskim komunikacijama (ZEK) istakao da je odstupanje od nepovredivosti tajnosti komunikacije po Ustavu Republike Srbije moguće samo u slučajevima kada to zahteva vođenje krivičnog postupka ili očuvanje nacionalne bezbednosti. U Nacrtu izmena i dopuna ZEK-a pored ovih dodata su i odstupanja u slučajevima vođenja istrage ili otkrivanja krivičnog dela kao i očuvanju javne bezbednosti što je mnogo širi pojam od nacionalne i prevazilazi ograničenja koja Ustav dozvoljava u celoj ovoj odredbi.

Ukoliko se ovakve i slične primedbe ne usvoje, Zakon će ostati u koliziji sa Ustavom.

Bezbednosno-informativna agencija (BIA)

Neki pomaci u ovom smeru su već načinjeni. Naime, u avgustu 2012. godine, na preporuku Ombudsmana, Bezbednosno-informativna agencija (BIA) uvela je takozvani „dupli" ili "dvostruki ključ" za pristup komunikacijama građana. „Dvostruki ključ" onemogućava da se samo sa jednog mesta aktivira prisluškivanje bilo čijeg telefonskog broja, što konkretno znači da niko u Agenciji neće moći da aktivira prisluškivanje nečijeg telefona na svoju ruku, već samo u "sadejstvu" sa osobom koja je ovlašćena da tu meru odobri, čime će mogućnost zloupotrebe elektronskog nadzora komunikacija građana biti svedena na još manju meru.

Kako je i ranije navedeno, u izveštaju evropskog eksperta Mauricija Varanezea o proceni rada službi bezbednosti u Srbiji iz marta ove godine navodi se da BIA zapravo funkcioniše kao *provajder* za sve druge službe, odnosno da uvek kada policija ili VBA žele da izvrše presretanje komunikacije u svrhe istrage, sudski nalog se uručuje BIA ili VBA, koji preko tehničke opreme koju poseduju dupliraju i usmeravaju telefonsku liniju prema Službi za

specijalne istražne metode (SSIM) u Upravi kriminalističke policije, koja od pre nekog vremena vrši stvarno presretanje telefonskih razgovora.

Nedavno je Ustavni sud Srbije proglasio neustavnim tri odredbe Zakona o Bezbednosno-informativnoj agenciji koje se tiču prisluškivanja i nepovredivosti tajnosti pisama. U odluci se navodi da je Ustavni sud utvrdio da odredba člana 13. Zakona o BIA, kojom je propisano odstupanje od načela nepovredivosti tajnosti pisama i drugih sredstava opštenja, nije u saglasnosti sa Ustavom, jer nije formulisana dovoljno jasno i precizno. Osporeni član glasi: „Direktor Agencije može, ako je to potrebno iz razloga bezbednosti Republike Srbije, svojim rešenjem, a na osnovu prethodne odluke suda, odrediti da se prema određenim fizičkim i pravnim licima preduzmu određene mere kojima se odstupa od načela nepovredivosti tajne pisama i drugih sredstava opštenja, u postupku utvrđenom ovim zakonom“. Sud je ocenio da ni osporene odredbe člana 14. i člana 15. Zakona nisu saglasne s Ustavom, jer su u pravnoj i logičkoj vezi sa odredbama člana 13. koje su prethodno ocenjene kao neustavne - navodi se u odluci. Međutim, objavljivanje te odluke je odloženo za šest meseci, umesto za četiri meseca kako je prvobitno bilo određeno odlukom Ustavnog suda.

Sud je doneo takvu odluku na zahtev skupštinskog Odbora za ustavna pitanja i zakonodavstvo, imajući u vidu da je u međuvremenu raspuštena Skupština Srbije, a, po Ustavu, raspušteni parlament može da obavlja samo tekuće poslove.

"To znači da do konstituisanja nove Narodne skupštine objektivno nije moguće odgovarajućom izmenom Zakona otkloniti utvrđenu neustavnost", rekli su u Ustavnom sudu.

Vojne službe

Dalje, u februaru 2013. godine, usvojen je i Zakon o izmenama i dopunama Zakona o Vojno-bezbednosnoj i Vojnoobaveštajnoj agenciji. Nakon odgovora Ustavnog suda na Zahtev za ocenu ustavnosti koji su Ombudsman i Poverenik podneli, a koji je dva člana Zakona o Vojno-bezbednosnoj i Vojnoobaveštajnoj agenciji proglasio neustavnim, utvrđeno je da direktor Vojnobezbednosne agencije (VBA) može da daje nalog za tajni elektronski nadzor komunikacija samo uz odobrenje suda. Izmenama tog zakona utvrđeno je da viši sud na području apelacionog suda na kome se preduzma mera odobrava tajni elektronski nadzor telekomunikacija, čime se može videti “listing” – Član 12, stav 1, tačka 6 Zakona: *Tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju, bez uvida u njihov sadržaj;.*

Precizirano je da se posebni postupci i mere preduzimaju na osnovu pisanog i obrazloženog naloga direktora VBA ili lica u VBA koga ovlasti direktor te agencije, a o izdatim nalozima se vodi evidencija. To je amandmanom tražila Demokratska stranka Srbije. Utvrđeno je da sudija višeg suda u sedištu apelacionog suda donosi odluku za primenu posebne mere bez odlaganja, a najkasnije u roku od osam sati. Pored bezbednosne zaštite informaciono-telekomunikacionih sistema, VBA će nastavi da pruža i kriptozaštitu.

Usvojenim amandmanom ombudsmana Saše Jankovića utvrđeno je da ako VBA ili VOA dođe u posed podataka i informacija iz nadležnosti drugih službi bezbednosti ili policije, te podatke i informacije dostaviće drugim službama bezbednosti ako su od značaja za nacionalnu bezbednost, a policiji ako se odnose na krivična dela na koja se, u skladu sa odredbama Zakonika o krivičnom postupku, primenjuju posebne dokazne radnje.

Odbor za kontrolu službi bezbednosti Skupštine Srbije nedavno je usvojio šestomesečni Izveštaj o radu Vojnobezbednosne agencije. Članovi Odbora pozitivno su ocenili profesionalno postupanje i rad pripadnika te agencije na ostvarivanju prioritetnih zadataka a naglašena je i puna podrška njihovom daljem angažovanju na realizaciji težišnih zadataka bezbednosne i kontraobaveštajne zaštite Ministarstva odbrane i Vojske Srbije, kao i u suprotstavljanju organizovanom kriminalu i korupciji.

Zakon o krivičnom postupku (ZKP)

Ombudsman i Poverenik podneli su i zahtev Ustavnom sudu da se proglasi neustavnim član 282 i 283/6 ZKP-a koji predviđju da tužilaštvo može "podneti zahtev državnim i drugim organima i pravnim licima da mu pruže potrebna obaveštenja". S tim u vezi, uz uslov da se ta zakonska norma korektno tumači, ne bi trebalo da bude bilo šta sporno, ali, korektno tumačenje nužno podrazumeva da mora biti nesporno da se ta norma ne odnosi na podatke koji su predmet posebnih ustavnih garancija ljudskih prava i koje bilo kome, pa razume se i tužilaštvu, mogu biti dostupni samo pod uslovima i na način utvrđen Ustavom. i Po nalogu javnog tužioca policija može u cilju ispunjenja dužnosti iz stava 1. ovog člana pribaviti evidenciju ostvarene telefonske komunikacije, korišćenih baznih stanica ili izvršiti lociranje mesta sa kojeg se obavlja komunikacija.

To izvesno važi za listing komunikacija fizičkog lica, na koji se odnose ustavne garancije o tajnosti pisma i drugih sredstava komuniciranja iz člana 41. Ustava. Pristup ovim podacima, po izričitoj odredbi Ustava, dozvoljen samo na osnovu odluke suda. Zato zahtevi tužilaštva usmereni na pribavljanje ovakvih podataka bez odluke suda, pritom još propraćeni stavljanjem u izgled novčanih kazni predstavljaju prekoračenje ovlašćenja koje tužilac ima po ZKP-u i istovremeno kršenje navedenih ustavnih garancija. Ustavni sud do danas o ovome nije odlučivao. Da bi se napravili koraci ka implementaciji predloženih mera Ombudsmana i Poverenika, neophodno je da Ustavni sud da proglasi neustavnim sporne odredbe Zakonika o krivičnom postupku, kako bi princip procesnih garancija iz člana 41. Ustava Republike Srbije bio dosledno prenet u svim zakonima koji uređuju pristup zadržanim podacima.

Prema tome policija je jedina služba bezbednosti u Srbiji kojoj Zakon, u koliziji sa Ustavom daje mogućnost pristupa informacijama i prisluškivanja. Samim tim, tehnički je neizvodljivo ujediniti agencije i policiju u jednu nacionalnu agenciju ako ne važe isti zakoni za sve, odnosno ukoliko se ne sprovede neophodna reforma sektora bezbednosti, kako bi se Zakoni iz ove oblasti usaglasili kako međusobno tako i sa, što je najvažnije, Ustavom.

Ostale mere

Da bi se obezbedilo i efikasno sprovođenje navedenih zakona, kao i funkcionisanje nadležnih službi, ova zakonska rešenja moraju biti propraćena odgovarajućim organizacionim merama poput 24-časovnog namenskog dežurstva sudija i informatičkih rešenja koja bi ubrzala prethodnu sudsku kontrolu i odlučivanje o zahtevima za pristup komunikacijama i podacima o komunikacijama.

Zaključak

Posledice navedenih odluka Ustavnog suda su višestruke. Pre svega, nesporno je da će ubuduće službe bezbednosti, organi odbrane i unutrašnjih poslova, moći da prikupljaju i

pristupaju podacima samo na osnovu predhodne odluke suda. Pored toga, sva pitanja vezana za zadržane podatke će morati da se regulišu zakonom a ne podzakonskim aktom. Takođe, ove dve odluke zahtevaće potpuno usaglašavanje ZKP - a sa Ustavom.

Potrebno je, dakle, najpre urediti problem presretanja komunikacija i drugih signala BIA, VOA i VBA kao i samoj policiji, pre nego što se krene dalje ka razvoju jedne, nacionalne agencije koja će sprovoditi ove mere. Imajući ovaj problem u vidu, kao smernica za dalje korake može da posluži dokument koji su sačinile svetske organizacije koje se bave principom prava na privatnost – civilno društvo i stručnjaci za oblast privatnosti i tehnologije - pod nazivom Međunarodni principi o primeni ljudskih prava na nadzor komunikacija (International Principles on the Application of Human Rights to Communications Surveillance). Principi su objavljeni paralelno sa izveštajem specijalnog izvestioca Ujedinjenih nacija o slobodi mišljenja i izražavanja, koji se detaljno bavi pitanjima široke upotrebe državnog nadzora komunikacija, zaključujući da takav nadzor ozbiljno narušava pravo građana na privatni život, slobodno izražavanje i druga, fundamentalna ljudska prava. Potrebu za iznalaženje optimuma (ravnoteže) u primeni ustavom zagarantovanih ljudskih prava i ustavom zagarantovane bezbednosti građana nedavno je istakla i Visoka komesarka UN za ljudska prava.

Prema Međunarodnim principima o primeni ljudskih prava na nadzor komunikacija građana, prilikom usvajanja novih tehnika nadzora i pristupa elektronskim komunikacijama ili proširivanja postojećih tehnika, država treba da pre pristupa informacijama utvrdi da li se one kvalifikuju kao "zaštićene informacije" i da li postupak nadzora treba da bude predmet sudskog ili drugog demokratskog kontrolnog mehanizma, odn. na koji način se one koriste. Prilikom razmatranja da li podaci dobijeni putem nadzora i pristupa elektronskim komunikacijama potpadaju pod "zaštićene informacije", forma, obim i trajanje nadzora su relevantni činioci. S obzirom da sveobuhvatno i sistematsko praćenje može otkriti privatne informacije u obimu koji daleko prevazilazi koncept sastavnih delova samih informacija koje su dostupne, potrebno je podići nivo nadzora nezaštićenih delova komunikacije na nivo koji podrazumeva snažnu zaštitu.

Određivanje da li država može sprovesti nadzor i pristup elektronskim komunikacijama ako na taj način zadire u zaštićene podatke mora obratiti pažnju na sledeće principe:

- **Zakonitost**: Bilo kakvo ograničenje prava na privatnost mora biti propisano zakonom.
- **Legitiman cilj**: Zakon bi trebalo da dopusti nadzor i pristup elektronskim komunikacijama jedino od strane tačno utvrđenih državnih organa ako je nadzor kao mera neophodan u demokratskom društvu radi zaštite zakonom utvrđenih legitimnih ciljeva.
- **Neophodnost**: Zakoni koji dozvoljavaju nadzor i pristup elektronskim komunikacijama od strane države se moraju ograničiti na nadzor koji je neophodan i jasno usmeren ka ostvarivanju legitimnog cilja.
- **Adekvatnost**: Svaka mera nadzora i pristupa elektronskim komunikacijama, omogućena u skladu sa zakonom, na svakom nivou mora da bude prikladna za ostvarivanje legitimnog cilja.
- **Proporcionalnost**: Odluke kojima se propisuju mere nadzora i pristupa elektronskim komunikacijama moraju da budu takve da uspostave balans između

legitimnog interesa koji žele da postignu i moguće povrede individualnih prava i drugih interesa do kojih može da dođe u primeni tih mera, a imajući u vidu i osetljivost informacija i ozbiljnost povrede u odnosu na pravo na privatnost.

- **Nadležnost sudskog organa**: Odluke u vezi sa nadzorom i pristupom elektronskim komunikacijama mora da donese nadležan sud koji je nezavisan i nepristrasan.
- **Postupak pred sudom**: Sudski postupak zahteva da države članice poštuju ljudska prava, tako što će obezbediti da je bilo koje ograničavanje ljudskih prava taksativno propisano u zakonu, da se dosledno sprovodi u praksi i da je javno dostupno.
- **Korisnička obaveštenja**: Lica bi trebalo da budu obaveštena o odluci odobravanja nadzora i pristupa elektronskim komunikacijama, kako bi im se u razumnom roku omogućilo da se žale na odluku kojom je odobren nadzor elektronskih komunikacija, a trebalo bi i da im se omogući pristup dokumentima na kojima se temelji donošenje te odluke.
- **Transparentnost**: Države bi trebalo da omoguće operatorima da objave procedure koje primenjuju kada se radi o državnom nadzoru i pristupu elektronskim komunikacijama, koliki je stepen pridržavanja tih procedura, kao i podatke o državnom nadziranju i pristupu elektronskim komunikacijama.
- **Javni nadzor**: Države treba da ustanove nezavisne mehanizme kontrole nad primenom mera nadzora i pristupa elektronskim komunikacijama, kako bi osigurale transparentnost i predvidivost ovog nadzora.
- **Integritet komunikacija sistema**: Kako bi osigurali integritet, sigurnost i privatnost elektronskog nadzora, uzimajući u obzir činjenicu da ugrožavanje sigurnosti u državne svrhe skoro uvek ugrožava sigurnost mnogo opštije, države ne smeju da prisiljavaju operatore ili prodavce hardvera i softvera da ugrađuju elektronski nadzor ili funkcije praćenja u svoje sisteme, niti da prikupljaju ili zadržavaju određene informacije isključivo za svrhe državnog nadzora.
- **Zaštitne mere za međunarodnu saradnju**: Sporazumi o međunarodnoj pravnoj pomoći (MLATs) i drugi sporazumi koje država zaključuje, treba da osiguraju da kada na nadzor i pristup elektronskim komunikacijama mogu biti primenjeni zakoni više država, merodavno bude pravo koje obezbeđuje viši nivo zaštite za pojedince. Kada države traže pomoć u svrhu primene zakona, princip dvojnog kriminaliteta treba primeniti.
- **Mere zaštite od nezakonitog pristupa**: Države treba da donesu zakone koji će inkriminisati nezakonit nadzor i pristup elektronskim komunikacijama od strane državnih organa ili privatnih lica. Zakon treba da obezbedi odgovarajuće i značajne građanske i krivične sankcije, zaštitu za uzbunjivače i pravna sredstva za obeštećenje oštećenih lica. Zakon treba da utvrdi da bilo koja informacija dobijena na način koji je u suprotnosti sa ovim principima ili ako je izvedena iz informacije koja je suprotna ovim principima, bude neprihvatljiva kao dokaz u bilo kom postupku. Države bi trebalo da donesu zakone koji će obezbediti da, nakon što je materijal koji je dobijen kroz elektronski nadzor i upotrebljen u svrhe za koje je informacija i data, bude uništen ili vraćen licu koje je bilo subjekt nadzora.

TAČKA 5: UJEDINITI PROCEDURE PREMA PRUŽAOCIMA USLUGA ELEKTRONSKIH KOMUNIKACIJA

Ujediniti procedure prema pružaocima elektronskih komunikacija i njihove obaveze

Pravo na privatnost je fundamentalno ljudsko pravo od ključnog značaja u demokratskim društvima. Ovo pravo je neophodno za poštovanje ljudskog dostojanstva i predstavlja preduslov za poštovanje drugih prava, poput prava na slobodu izražavanja i informisanja i prava na slobodu udruživanja, a garantovano je i međunarodnim sporazumima iz oblasti zaštite ljudskih prava. Mere koje se primenjuju u oblasti nadzora i pristupa elektronskim komunikacijama, a kojima se ograničava pravo na privatnost, mogu biti opravdane jedino ako su propisane zakonom, ako su neophodne za postizanje legitimnog cilja i ako su srazmerne tom cilju.

Međutim, u Srbiji ne postoji nijedan pravilnik ili kodeks, niti bilo kakve smernice koje bi omogućile pružaocima usluga da se pozovu na njih u slučaju da sumnjaju da bi saradnja sa bezbednosnim službama uslovila kršenje zakona.

U Zakonu o elektronskim komunikacijama stoji samo da „presretanje elektronskih komunikacija kojim se otkriva sadržaj komunikacije nije dopušteno bez pristanka korisnika, osim na određeno vreme i na osnovu odluke suda, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom“. (član 126. Zakona o elektronskim komunikacijama) Uprkos tome, Zakon ne sadrži bliže specifične odredbe koje bi bile standardizovane i kojih bi se pružaoci usluga elektronskih komunikacija mogli pridržavati.

Neophodno je naglasiti da Srbija nije jedina koja zemlja koja je suočena sa ovim problemom. Kompanije koje se bave informacionim i komunikacionim tehnologijama širom sveta suočene su sa pojačanim pritiskom od strane države da se povinuju zahtevima koji su neretko u sukobu sa međunarodno priznatim standardima ljudskih prava na privatnost i slobodu izražavanja. Usled nepostojanja jasnih smernica, regulacija i zakonskog okvira, ostaje mogućnost da se pružaoci usluga elektronskih komunikacija udruže u vidu samoregulacije sektora i time izvrše pritisak na Vladu da se naprave koraci ka potpunom usvajanju ove tačke**.**

Jedno od mogućih rešenja dolazi u obliku preporuka koje je sastavila multi-dimenzionalna grupa kompanija, organizacija civilnog društva, investitora i akademika koji su osnovali Inicijativu Globalna mreža, za zaštitu i unapređenje slobode izražavanja i privatnosti u okviru informaciono-komunikacionih tehnologija. Inicijativa je izdala vodič za implementaciju principa slobode izražavanja i privatnosti, namenjen svim zainteresovanim stranama, povezanim sa industrijom informaciono-komunikacionih tehnologija, koji opisuje niz koraka da bi ostvarilo usklađivanje sa principima, kao i niz koraka za njihovo sprovođenje.

U skladu sa ovim principima, pružaoci elektronskih komunikacija su između ostalog upućeni da:

- *Prvenstveno procene uticaj ljudskih prava na tržište, proizvode, tehnologije i usluge koje pružaju, a koje predstavljaju najveću pretnju za slobodu izražavanja i privatnost, na ljudska prava*
- *Ažuriraju ove procene uticaja ljudskih prava redovno, kada dođe do značajnih izmena zakona, propisa, tržišta, proizvoda, tehnologija ili usluga*
- *Koriste pogodnosti koje pruža saradnja sa grupama za ljudska prava, državnim organima, međunarodnim organizacijama i materijale nastale kroz ovakvu saradnju*
- *Uključe nalaze procene uticaja ljudskih prava u druge aktivnosti, kao što je procena korporativnog rizika*.

Kompanije bi, dakle, udruženim snagama trebalo da podstaknu državu da bude transparentna i dosledna u zahtevima, zakonima i propisima i da zahtevi budu u skladu sa međunarodnim pravom i standardima. Sledeći korak bilo bi usvajanje politike i uspostavljanje procedura, odnosno načina na koji će pružaoci elektronskih usluga proceniti i odgovoriti na zahteve državnih službi za pristup ličnim podacima. Pružaoci bi, prema tome, zahteve trebalo da tumače usko i sprovode samo one koji ostavljaju prostor za očuvanje privatnosti; zahtevaju pojašnjenje ili izmenu zahteva kada se čini da on prevazilazi nadležnosti, da je nezakonit, da ne ispunjava zakonsku regulativu ili da nije u skladu sa međunarodnim standardima ljudskih prava i standardima koji se odnose na privatnost.

Poverenik i Ombudsman su predložili u cilju efikasnijeg sprovođenja i bolje kontrole zakonitosti mera nadzora da je potrebno i na normativnom i na faktičkom planu stvoriti uslove za ujedinjenje postojećih paralelnih i multiplikovanih tehničkih mogućnosti različitih agencija i policije u jednu, nacionalnu agenciju koja, kao provajder, pruža tehničke usluge neophodne za presretanje komunikacija i drugih signala svim autorizovanim korisnicima. Time bi se, dugoročno, ujednačile procedure prema pružaocima elektronskih komunikacija i njihove obaveze i obezbedilo neizbrisivo beleženje pristupa telekomunikacijama, uz sve podatke koji su potrebni da bi se ozbiljno mogla vršiti naknadna kontrola zakonitosti i pravilnosti pristupa. U međuvremenu, samoregulacija, u saradnji sa drugim zainteresvanim stranama, poput civilnih društava, akademika, investitora i slično, deluje kao najviše održiva opcija u ovom trenutku.

TAČKA 10: OBAVEZATI UNUTRAŠNJE NADZORNE MEHANIZME DA O SVOJIM NALAZIMA OBAVEŠTAVAJU ZAŠTITNIKA GRAĐANA

Obavezati unutrašnje nadzorne mehanizme da o svojim nalazima od značaja za poštovanje ljudskih prava obaveštavaju Zaštitnika građana i nadležne skupštinske odbore, posebno u slučajevima kada se o njih oglušilo rukovodstvo organa u kojima su obrazovani i u slučajevima koji govore o ozbiljnim navodnim ili potvrđenim kršenjima ljudskih prava

Uspostavljanje sistema u kojem bi nadzorni mehanizmi unutrašnje kontrole direktno bili upućeni na saradnju sa Kancelarijom Ombudsmana i Poverenika u svrhu ostvarivanja potpune zaštite ličnih podataka i podataka od javnog značaja, predstavlja fundamentalni korak ka njihovom institucionalnom jačanju. Međutim, u sprovođenju ove tačke postoje dva problema.

Prvo, najveći otpor ka implementaciji ove tačke dolazi iz samih državnih institucija. Činjenica da one svoje unutrašnje kontrolne mehanizme smatraju, upravo, *svojim*, uslovljava i to da nezavisne kontrolne mehanizme, poput Ombudsmana i/ili Poverenika vide kao potencijalnu pretnju.

Sa druge strane, uprkos medijskoj pažnji koju institucije Ombudsmana i Poverenika uživaju, čini se da nadležne institucije, ali i organizacije i kompanije (poput pružalaca usluga elektronskih komunikacija) nisu dovoljno upoznate sa zakonskim okvirom u kojem Ombudsman i Poverenik rade. Ova tvrdnja dokazana je i činjenicom da su, kako je Ombudsman i sam naglasio, neki pružaoci elektronskih komunikacije (operateri), uprkos usvojenom Zakonu o Zaštitniku građana, smatrali da moraju da pitaju Bezbednosno-informativnu agenciju da li im je dozvoljeno da, kao nezavisnom, kontrolnom državnom organu, ustupe prikupljene podatke.

Drugo, tematika tačke je usko povezana sa pitanjem zaštite uzbunjivača, na koju se Ombudsman i Poverenik takođe ukazali u tački 8 liste 14 predloga, pozivajući na potrebu da se „omogući jaka pravna i faktička zaštita uzbunjivača“. Uprkos činjenici da Zakon o Zaštitniku građana određuje da Zaštitnik građana ima pravo da obavi razgovor sa *svakim* zaposlenim u organu uprave kada je to od značaja za postupak koji se vodi, ovakva praksa često nije slučaj jer je to onemogućeno ili zato što zaposleni ne žele da sarađuju usled nedostatka institucionalne zaštite uzbunjivača.

Zakon o zaštiti uzbunjivača uredio bi zaštitu lica koje, zbog osnovane sumnje na korupciju ili otkrivanja podataka o drugim štetnim ili potencijalno štetnim pojavama po zakonom zaštićeni javni interes, takve podatke prijave nadležnim državnim i nezavisnim organima.

Nedavno je zatvorena javna rasprava o radnoj verziji nacrta Zakona o uzbunjivačima koji je predložilo Ministarstvo pravde. Mišljenja smo, kao i većina nevladinog sektora, Poverenik i Ombdusman, da je radna verzija nacrta Zakona promašila intenciju i da ne pruža adekvatnu zaštitu uzbunjivačima, koja je potrebna zbog zaštite javnog interesa, a koji uzgred nije ni definisan u radnoj verziji Nacrta. Ostaje da vidimo koliko će se komentari uvažiti i hoće li se ovaj, veoma važan Zakon, doneti u skladu sa opštom intencijom.

ZAKLJUČCI I PREPORUKE

Analizom postojećeg zakonodavnog okvira utvrđeno je da je neophodno što pre regulisati oblast zaštite privatnosti i zaštite podataka o ličnosti građana Srbija, koja je trenutno u značajnom raskoraku sa ustavnim garancijama.

14 preporuka, odnosno tačaka, koje su Ombudsman Saša Janković i Poverenik za informacije Rodoljub Šabić izneli u julu 2012. godine, predstavlja početnu tačku koja čini osnovu uređenja ove oblasti, kako bi se omogućilo nesmetano korišćenje ustavom zagarantovanih ljudskih prava.

CEAS podseća da je, prema rezultatima istaživanja „Za dinamičniju reformu sektora bezbednosti u Srbiji“ o stanju u sektoru bezbednosti i daljim neophodnim reformskim koracima, sprovedenog u okviru projekta: „Vreme je: Zagovaranje nastavka reforme sektora bezbednosti u Srbiji“ tokom novembra 2012. godine, angažovana javnost u okviru ciljne grupe (uključujući narodne poslanike, državne službenike i civilno društvo) izrazila interesovanje da se ova oblast uredi. Nažalost, politička elita ni tada, kao ni sada, nije pokazala dovoljno političke volje da ovo pitanje stavi na dnevni red.

CEAS smatra da je neophodno doneti poseban Zakon o bezbednosnim kako bi se, pre svega, ocene, to jest zaključci koji proizilaze iz bezbednosnih provera fizičkih lica, stavili pod demokratsku kontrolu, sa ciljem da se na pouzdan način spreče moguće zloupotrebe.

CEAS podržava predlog od 14 tačaka u potpunosti i poziva nadležne institucije da što pre usvoje predviđene uredbe i pravilnike, kako bi se obezbedila implementacija zakona koji regulišu ovu oblast.

CEAS smatra da očekivani početak pregovora sa Evropskom unijom i otvaranje poglavlja 23 - Reforma pravosuđa i osnovna prava i 24 – Pravda, sloboda i bezbednost, ali i 32 – Finansijska kontrola, otvara mogućnost da Zapadna međunarodna zajednica izvrši dodatni pritisak na političku elitu u Srbiji da se ova oblast uredi u potpunosti.

CEAS pozdravlja saradnju vojnih službi bezbednosti, tačnije, Vojnobezbednosne i Vojnoobaveštajne agencije sa Ombudsmanom i Poverenikom.

CEAS pozdravlja i saradnju Bezbednosno-inofrmativne agencije sa sa Ombudsmanom i Poverenikom.

CEAS se nada da će na isti način i Ministarstvo unutrašnjih poslova postupiti u skladu sa podrškom Ombudsmanu i Povereniku, koju je ministar Ivica Dačić javno iskazao, i što pre sprovesti potrebne mere kako bi se oblast nadzora i pristupa elektronskim komunikacijama građana regulisala i u okviru ove službe sistema bezbednosti.

CEAS podržava aktivnosti Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka pravcu normativnog regulisanja oblasti zaštite tajnosti podataka.

CEAS je, nakon iscrpnih konsultacija sa Ombudsmanom i Poverenikom, i ostalim predstavnicima ovih institucija, kao i konsultacijama sa Kancelarijom Saveta za nacionalnu bezbednost i zaštitu tajnih podataka formirao sledeće kratkoročne preporuke:

- Izmeniti Zakon o elektronskim komunikacijama nakon odluke Ustavnog suda da su odredbe 128. i 129. koje se odnose na pristup zadržanim podacima mimo odluke

suda i na ovlašćenje nadležnog ministarstva da bliže uređuje zahteve u vezi sa zadržanim podacima podzakonskim aktom - neustavne;

- Izmeniti Zakonik o krivičnom postupku koji predviđa da tužilaštvo može "podneti zahtev državnim i drugim organima i pravnim licima da mu pruže potrebna obaveštenja";

- U zadatom roku uskladiti sporne odredbe zakona o BIA, koje je Ustavni sud Srbije proglasio neustavnim, a koje se odnose na tajnost pisma i bliže definisanje kategorije lica prema kojima se mogu primenjivati posebne mere nadzora (uključujući prisluškivanje po nalogu suda)

- Urediti pitanje presretanja elektronskih komunikacija građana u policiji kako bi to pitanje postalo regulisano u svim službama sistema bezbednosti Srbije;

- Podstaći pružaoce usluga elektronskih komunikacija na bližu saradnju i samoregulaciju, kako bi se razvio jedinstveni standard kojeg se pridržavaju svi pružaoci usluga;

- Usvojiti adekvatan Zakon o zaštiti uzbunjivača koji bi im pružio i pravnu i faktičku zaštitu kako bi se omogućio siguran pravni okvir za saradnju sa institucijama Ombudsmana i Poverenika.

- Doneti poseban Zakon o bezbednosnim proverama

- Otkloniti uočene manjkavosti i pravne praznine postojećeg Zakona, kao i stvaranje uslova za efikasniju primenu samog Zakona

- Edukovati organe javne vlasti sa Zakonom o tajnosti podataka, i uskladiti normativu u smislu terminologije i postupanja sa tajnim podacima uopšte.

Ovo bi omogućilo ostvarenje nekih od dugoročnih ciljeva poput:

- **Sjedinjavanja svih paralelnih tehničkih mogućnosti za presretanje komunikacija i drugih signala u jednu nacionalnu agenciju (tačka 4);**

- **Ujedinjavanja procedura prema pružaocima elektronskih komunikacija (tačka 5);**

- **Saradnju mehanizama unutrašnje kontrole sa institucijom Ombudsmana i Poverenika (tačka 10).**

CEAS će nastaviti da u okviru svojih aktivnosti, kako na ovom tako i na drugim projektima, prati dešavanja u ovoj oblasti.

ANEKS I: Inicijativa Poverenika za informacije oid javnog značaja i zaštitu podataka o ličnosti za donošenje Zakona o bezbednosnim proverama upućena Vladi Republike Srbije 15. oktobra 2012. godine

Република Србија
Повереник за информације
од јавног значаја и заштиту
података о личности
Светозара Марковића 42
11000 Београд

Тел: +381 (0) 11 3408-900
Факс:+381 (0) 11 2685-023
office@poverenik.rs
www.poverenik.rs
Адреса за пошту:
Немањина 22-26, Београд

Број: 011-00-685/2012-01 Датум: 15.10.2012.

ВЛАДА РЕПУБЛИКЕ СРБИЈЕ

11000 Београд
Немањина 11

На основу сагледавања закона и других прописа којима се уређује материја безбедносних провера, на основу поступака вођених по представкама грађана, а у складу са чланом 44. став 1. тачка 1. и тачка 11. Закона о заштити података о личности ("Сл. гласник РС", бр. 97/2008, 104/2009 - др. закон и 68/2012-одлука УС), Повереник за информације од јавног значаја и заштиту података о личности подноси

ИНИЦИЈАТИВУ
ЗА ДОНОШЕЊЕ ЗАКОНА О БЕЗБЕДНОСНИМ ПРОВЕРАМА

Оцењујући да је из више разлога потребно да се материја безбедносних провера у Републици Србији уреди на јединствен и целовит начин подносим Влади Републике Србије Иницијативу да у складу са њеним овлашћењима из члана 123. тачка 4. Устава Републике Србије припреми и с предлогом за усвајање поднесе Народној скупштини Репубике Србије Закон о безбедносним проверама.

Према садашњем стању ствари, Устав Републике Србије („Сл. гласник РС“ бр. 83/2006) утврђује да Република Србија уређује и обезбеђује безбедност Републике Србије (члан 97, тачка 4). Закон о основама уређења служби безбедности Републике Србије („Сл. гласник РС“, бр. 116/2007 и 72/2012) уређује субјекте безбедносно-обавештајног система у нашој

држави, питање усмеравања и усклађивања рада служби безбедности, као и надзора над њиховим радом, али не и материју безбедносних провера.

Материја безбедносних провера уређена је у неколико закона и других прописа, али на неодговарајући начин. Разлог томе је што се вршење безбедносних провера уређује само у контексту материје која се непосредно уређује предметним законима и другим прописима. То су по правилу они закони, односно други прописи којима се уређује материја запошљавања у државним органима, нарочито у полицији, војсци и службама безбедности, као и материја школовања у школским установама које су проходне за запошљавање у наведеним државним органима.

Тако нпр. Закон о тајности података ("Сл. гласник РС", бр. 104/2009) садржи одредбе које предматну материју уређују свеобухватније него остали закони, али само у контексту приступа тајним подацима. Слично томе, Закон о организацији и надлежности државних органа у сузбијању организованог криминала и других тешких кривичних дела ("Сл. гласник РС", бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 - др. закон, 45/2005, 61/2005, 72/2009, 72/2011 - др. закон и 101/2011 - др. закон) уређује ово питање у односу на узан круг лица из веома малог броја правосудних органа, и при том то чини нејасним и недовољно прецизним одредбама. Даље, одредбе Закона о полицији ("Сл. гласник РС", бр. 101/2005, 63/2009-одлука УС и 92/2011) садрже само уопштену дефиницију безбедносне сметње и уређују безбедносну проверу у контексту запошљавања у Министарство унутрашњих послова. На ове одредбе о вршењу безбедносне провере из Закона о полицији, позива се Одлука о оснивању Криминалистичко-полицијске академије ("Сл. гласник РС", бр. 58/2006), иако је ова академија високошколска установа а не организациони део МУП, и то приликом уређивања питања учешћа на конкурсу за пријем кандидата на школовање у овој установи. И у Војсци Србије се вршење безбедносних провера приликом запошљавања не уређује законом већ се непосредно уређује Правилником о безбедносним проверама лица које врши Војнобезбедносна агенција ("Сл. војни лист", бр. 18/2010).

Основни недостаци и спорна питања у вези са одредбама предметних и других ненаведених закона и других прописа, као и приликом њихове примене, су:

1. Материја безбедносних провера је већ деценијама уређена у Србији у неколико закона и других прописа, али само сегментарно, непотпуно и непрецизно;
2. Већина ових закона и прописа не садржи одредбе о основним појмовима, субјектима који се проверавају, сврси и поступку вршења провера, роковима, и др, што оставља исувише простора за дискрециono тумачење и поступање надлежних органа, чак и појединаца. У случају када предметни прописи садрже ове одредбе, онда су исте готово по правилу непотпуне и/или се односе искључиво на области које се непосредно уређују овим прописима;
3. Вишедеценијска примена ових, али и раније важећих прописа са истим или сличним решењима, доводила је и данас доводи до кршења људских права и слобода, посебно права на приватност, односно права на заштиту података о личности. Нпр. обрада података често се врши без законског основа или законитог пристанка лица чији се подаци обрађују; често се врши обрада података трећих лица, по правилу чланова породице, за

које лице чији се подаци обрађују не може да да сагласност; скоро без изузетка не поштују се одредбе Закона о заштити података о личности којима се уређује право на обавештење о обради података о личности, право на увид у исте, право на копију ових података и др, а за шта је законом предвиђена прекршајна, а у одређеним случајевима и кривична одговорност.

У циљу отклањања наведених недостатака, подносим ову иницијативу за доношење Закона о безбедносним проверама. Решења садржана у закону чије доношење иницирам требало би да омогуће надлежним органима да врше безбедносне провере у свим ситуацијама у којима се оцени и законом, у складу с Уставом (који у чл. 42. предвиђа да се „прикупљање, држање, обрада и коришћење података о личности уређују законом“, што безбедносне провере свакако јесу) предвиди да је то потребно, али би таква решења истовремено била усаглашена са Уставом Републике Србије, Законом о заштити података о личности, као и општеприхваћеним правилима међународног права.

Закон о безбедносним проверама требало би да у основи на јединствен и целовит начин, доследно уреди вршење безбедносних провера, а посебно следећа питања: дефиниција основних појмова, пре свега безбедносне провере и безбедносне сметње; врсте безбедносних провера које се врше; који подаци се проверавају, ко то чини и у којим ситуацијама; функције, положаји, односно личности који су субјекти провера; сврха вршења безбедносних провера; поступак вршења безбедносних провера; рокови вршења безбедносних провера; последице извршених безбедносних провера; начин и рокови чувања резултата извршених безбедносних провера, као и по потреби друга питања која би дефинисали представници надлежних министарстава односно органа.

ПОВЕРЕНИК

Родољуб Шабић

ANEKS II: Transkripti govora predstavnika institucija Republike Srbija na CEAS završnoj konferenciji „Uključimo se u globalnu debatu o balansu između bezbednosti i privatnosti“

Konferencija, na kojoj je predstvaljen ovaj dokument kao finalna verzija Akcionog plana javnog zagovaranja usvajanja 14 tačaka Ombudsmana i Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, održana je 31. marta 2014. godine. Osim članova CEAS tima, izlaganje na konferenciji imali su Saša Janković, Ombudsman, Aleksandar Resanović, zamenik Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti i Sanja Dašić iz Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka kao predstavnici institucija, kao i Dragiša Jovanović, nezavisni CEAS konsultant za bezbednost.

Slede transkripti njihovih izlaganja predstavnika institucija.

Saša Janković, Zaštitnik građana

Drago mi je što sam danas ovde sa vama. Prokomentarisao bih nekoliko stvari koje smo danas čuli. Prvo predlažem da iz diskursa lagano izbacimo ono što je spomenuto, a za šta verujem da predstavlja lažno pitanje, odnosno lažnu dilemu - o ravnoteži između *bezbednosti* i *ljudskih* prava. Nema bezbednosti tamo gde se ne poštuju ljudska prava, niti ima ljudskih prava u odsustvu bezbednosti građana. Bezbednost i ljudska prava nisu međusobno obrnuto proporcionalni, jačanje jednog nije na uštrb drugog, već obrnuto – jačanjem bezbednosti potpunije se ostvaruju i ljudska prava, a garancije ljudskih prava smanjuju opasnost (objektivnu i subjektivno shvaćenu) po vrednosti do kojih građani najviše drže, te je i bezbednost veća. Analiza pojmova „bezbednost“ i „ljudska prava“ će to lako pokazati. Svođenje bezbednosti na pretnje fizičkom postojanju je neprihvatljivo i opasno uprošćavanje. Dilema koju, međutim, zaista smatram legitimnom je potraga za ravnotežom između *efikasnosti* i *kontrole*. Da li ćemo radi efikasnosti pustiti službe da rade što je brže i više moguće pa to, eventualno, tek naknadno kontrolisati ili ćemo uspostaviti mehanizam kontrole u realnom vremenu ili bar blisko tome, jer je to danas tehnološki moguće bez opasnosti da će primena mehanizama kontrole mogla usporiti rad službe? Smatram da bi dilema između efikasnosti i kontrole mogla da se prevaziđe upravo zahvaljujući današnjim informatičkim i komunikacionim tehnologijama. Da li će jačanje kapaciteta i ovlašćenja službi biti praćeno proporcionalnim jačanjem kontrole ili ne? Smatram da je to, u najmanju ruku, logično. Da li ćemo službama dozvoliti neselektivan pristup u privatnost, kako bi iz analizirali ceo plast sena i u njemu eventualno našli iglu (što je, čini se, stav američkog obaveštajno-bezbednosnog aparata) ili će službe morati da pruže uverljivu sumnju da je određena slamka u stvari igla, da bi dobili dozvolu da je analiziraju (i sa njom neumitno sve slamke u njenom neposrednom okruženju) još je jedno od važnih pitanja.

Pomenuto je i da je prošla vlast, odnosno vlada, bila neefikasna po pitanju reforme sektora bezbednosti, ali, ja sam zaštitnik građana od 2008 godine, i ja ne vidim bitnu razliku po tom pitanju u prošlosti – sve dosadašnje Vlade imale su rezervisan stav prema demokratizaciji

sektora bezbednosti i sve, uključujući i ovu u tehničkom mandatu, teže da ovaj sektor ostave nereformisanim, a mehanizme kontrole inferiornim. Možda je neka Vlada bila efikasnija u težnjama da od sektora bezbednosti napravi represivniji aparat, sa manje elemenata kontrole.

Čuli smo i stav investitora, odnosno poslovnog sektora da treba raditi procenu uticaja *ljudskih prava* na *tržište*, a ja smatram to gledište izvrnutim.

Tvrdim da treba proceniti uticaj tržišta na ljudska prava i pravila i ponašanje tržišta prilagođavati tako da se što potpunije ostvaruju ljudska prava, a ne suprotno. Da se razumemo, nisu sve ljudska prava, nije ljudsko pravo nekoga da vozi BMW, zato što je video nekog drugog da ga vozi na reklami. Ljudska prava su elementarne stvari, koja čine naš život, dostojanstvo našeg života i budućnost ljudske zajednice. Od toga da li će se ljudska prava poštovati ili ne zavisi to da li će čovek za 50 godina živeti kao slobodno biće ili ne, a od poštovanja tržišnih pravila i uspeha na njemu zavisi da li će voziti trabant ili BMW. Ja nemam sumnju u to šta treba da bude veći prioritet i šta čemu treba da se prilagođava, ako neko već insistira da se ispituje odnos tih kategorija.

Dve godine prošle od kako smo Poverenik za slobodan pristup informacijama od javnog značaja i ja predložili 14 mera za unapređenje stanja u pogledu poštovanja garancija ljudskih prava u radu sektora bezbednosti. Mada, moram da kažem da neke od tih mera datiraju i od ranije. Na primer, zahtev da se Zakon o BIA uskladi sa Ustavom uputio sam još 2010 godine, a u drugom svojstvu, ne kao zaštitnik građana, ukazivao sam na nesaglasnost sa Ustavom još 2006. godine. Odredbe tog zakona o primeni posebnih mera su neustavne iz razloga koji je aktuelizovan kroz slučaj Šarić – zakon praktično i ne navodi koje su to mere koje BIA može da preduzme u slučaju da se steknu zakonom propisani uslovi, te se formalno i ne zna koji su to načini mešanja u ljudska prava iz domena privatnosti kojima služba pribegava. Te mere moraju biti propisane, a zakon određen kako bi ponašanje službi bilo predvidivo. Kada je prvi potpredsednik Vlade javno naveo koje je mere BIA primenjivala u slučaju Šarić, meni to kao organu koji štiti ljudska prava ne predstavlja problem, naprotiv, te mere bi trebale da budu upisane u Zakon. Ali nisu. One su opisane podzakonskim aktima, koji nose oznake poverljivost, dakle tajni su.

Konačno, jedna od javno pomenutih mera je *tajni pretres*. Ta mera se ne preduzima radi neposrednog hvatanja počinioca, njena svrha je nešto drugo – ulazak u prostor kada u njemu nema nikog, radi traganja za inkriminišućim dokazima ili željenim informacijama. Traga se na način da o tome ne ostaje dokaz niti sumnja da je bilo ko u prostoru boravio, a potraga se radi bez naloga suda i bez svedoka. Međutim, nakon što je donet Ustav iz 2006. godine, ulazak u stan radi pretresa moguć je samo po nalogu suda i u prisustvu dva svedoka. Međutim, nedavno je javno rečeno da se tajni pretresi i dalje vrše. To znači da je moguće da pripadnici BIA bez bilo čijeg znanja, tajno ulaze u stanove i tajno iz njih izlaze i da se nakon toga može desiti da u naknadnom pretresu, ovaj put u skladu sa Ustavom – dakle uz nalog suda i nepristrasne svedoke, u nekom prostoru bude nađen inkriminisani materijal, a da niko, pa ni sud, ne zna da je u tom prostoru prethodno boravila tajna služba. To je velika opasnost po integritet dokaza i objektivnost sudskog postupka i ta opasnost se mora otkloniti.

Navešću još jednu stvar – narodni poslanik je lišen slobode, a da mu predhodno NSRS nije skinula imunitet. Imunitet se ne daje zbog ličnog komoditeta već da osigura nesmetano vršenje najbitnijih državnih funkcija i da spreči bilo koga da zloupotrebom ovlašćenja onemogući nosioce tih funkcija da svoju dužnost obave nepristrasno i slobodno. Zamislite da u danu u kome se glasa o nepoverenju Vladi privremeno bude ograničena sloboda kretanja troje poslanika opozicije zbog navodnog saobraćajnog prekršaja – što je u praksi moguće.

Odredba ustava kaže – osoba sa imunitetom ne može biti pritvorena dok taj imunitet narodna skupština ne skine. Nezvanično obrazloženje koje sam čuo je da to „pritvaranje" treba tumačiti kao „određivanje mere pritvora", a ne lišavanje slobode kretanja. Dakle, neko smatra da Ustavom garantovani imunitet sprečava sudiju (jer sudija određuje pritvor) da imaocu imuniteta ograniči slobodu, a da je to istovremeno dozvoljeno tužiocu u saradnji sa policajcem! Da li to znači da mi postajemo policijska država?

Na kraju - o uzbunjivanju. Zakon koji kaže da se tužbom za zaštitu uzbunjivanja ne može štititi od akta poslodavca kojim je odlučeno o pravima i obavezama po osnovu rada nije zakon koji štiti uzbunjivače, već pamflet. Čemu zakon koji uzbunjivača ne može da zaštiti od odmazde u vidu otkaza, premeštaja na niže radno mesto, upućivanja na rad na udaljeno mesto… uzbunjivačima treba zaštita od toga, ne od poprekog pogleda. Ako je „politička volja" da uzbunjivače ne štitimo od onoga od čega se u 100% do sada poznatih slučajeva sastojala odmazda, onda ne treba da gubimo vreme na pisanje zakona. Istovremeno se javnosti plasira da se uzbunjivači štite i da ljudi treba da veruju sistemu. Ljudi u te pozive veruju, dolaze građani koji traže zaštitu, istragu...brojne su pritužbe iz policije, Vojske, tajnih službi. Zaštitnik građana, međutim, ni bilo koji drugi organ, nije stvarno u mogućnosti da tim ljudima pruži zaštitu. Ne mogu kao savestan čovek da im tražim materijal o uzbunjivanju, jer znam da im je radno mesto ugroženo, a ako govore istinu ja nemam mehanizam da ih zaštitim, niti mogu da ih uputim na onoga ko može. Zadnji primer dolazi sa univerziteta – navodno je u pitanju milionska korupcija, posle čijeg dokumentovanog prijavljivanja čovek bez ikakvog obrazloženja ostaje bez angažovanja na fakultetu. A ja moram da mu kažem da mi dokumenta ne daje jer ako pokrenem postupak kontrole neću moći da ga zasigurno zaštitim. Ako mi ne poveruje, ili ako nije izvanredno hrabar, pomisliće da ja, kao Zaštitnik građana, žmurim pred bezakonjem i žmurim na kršenje njegovih prava i javnog interesa, da sam deo pokvarenog dela sistema...

U svakom slučaju, bez usvajanja bar velike većine od pomenutih 14 mera, nećemo daleko stići.

S druge strane, siva slika iz Godišnjeg izveštaja ombudsmana za 2013. godinu može biti brzo izmenjena, Srbija to može. Ne trebaju nam treninzi, ljudi koji rade naopake stvari znaju da ih rade naopako. U pitanju je namera da se radi zlo, a ne neznanje. Namera usled saznanja da učinjeno zlo prečesto ima dobre posledice po onog ko ga čini, a loše po onog ko mu se usprotivi. Najveći broj ljudi nije u situaciji da odbije nezakonito naređenje nadređenog, što zakon nalaže, ako znaju da time žrtvuju svoju karijeru, ekonomski položaj, porodicu, opstanak. Ni jedan sistem ne može da se zasniva na herojstvu.

Dakle, u Srbiji ima znanja, može se doći do odličnih rešenja. Pitanje je samo da li će nova Vlada Srbije kapacitet koji postoji u zemlji želeti da stavi u funkciju, ili ćemo se mi i dalje ovako skupljati i pričati stvari koje će voda da odnese.

Aleksandar Resanović, zamenik Poverenika za informacije od javnog značaja i zaštite podataka o ličnosti

Povodom sastavljanja spiskova nepodobnih i poziva na linč Žena u crnom:

Složio bih se s onim što je G - din Janković rekao i dodao bih da ovo nije prvi put da se kod nas prave tzv. spiskovi nepodobnih. Naime, i u prošlim vremenima pravile su se tzv. crne liste nepodobnih i neposlušnih, bazirane na političkoj, nacionalnoj, verskoj i/ili ideološkoj osnovi. Znači, ovi spiskovi su poziv na linč lica čija su imena na spisku, ali i svojevrsna opomena, bolje rečeno pretnja, svima koji misle isto kao i lica sa spiska.

Nesporno je da bi sastavljanja bilo kakvih spiskova nepodobnih trebalo da pripada nekim prošlim vremenima. Pravljenje spiskova je svojstveno autoritarnim režimima, kao što je krajem dvadesetog veka bio režim u Srbiji, odnosno njegovom predhodniku, totalitarnom komunističkom režimu. Pravljenje takvih spiskova nikako ne bi trebalo da bude svojstveno sistemu koji se naziva demokratskim.

Ovo je jedan globalni osvrt na nepoštovanje ljudskih prava, a sa aspekta nadležnosti Poverenika za informacije od javnog značaja i zaštite podataka o ličnosti mogao bih da ukažem na određene nezakonitosti. Naime, Zakon o zaštiti podataka o ličnosti uređuje da je obrada podataka o ličnosti dozvoljena ako za to postoji odgovarajući osnov u zakonu, a ne u podzakonskom aktu, ili da su lica čiji se podaci obrađuju dala saglasnost za to. S obzirom da u ovom slučaju nema ni jednog od ova dva pomenuta osnova, to i radnja obrade, odnosno formiranje predmetnih spiskova sa ličnim imenima i nekoliko drugih podataka koja ta lica čine određenim ili barem odredivim, nije dozvoljeno.

Prelazim na temu iz današnjeg programa

Osvrnuo bih se na neke navode koji su pominjani u analizi CEAS i na ovom skupu. Dozvolite mi da se kao prvo vratim korak unazad i ukažem na ono što je dovelo do 14 mera. Naime, Poverenik je izvršio nadzor nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane sva 4 operatera mobilne i fiksne telefonije u Srbiji – Telekoma, Telenora, VIP i Oriona, u periodu mart - juli 2012 godine. Predmet nadzora bilo je postupanje samo sa zadržanim podacima o ostvarenim komunikacijama, a ne i postupanje sa sadržinom komunikacije, i to za period od godinu dana unazad od vremena vršenja nadzora. Činjenica je da se analizom i ukrštanjem zadržanih podataka, a pogotovo u dužem vremenskom periodu, koji može da bude od 6 do 12 meseci, može nekada dobiti više informacija nego iz samog sadržaja ostvarene komunikacije. Želeli smo da vidimo da li se pre svega poštuju odredbe našeg Ustava, da li se istovremeno poštuju i opšteprihvaćena pravila međunarodnog prava na šta upućuje naš Ustav, ima li ostupanja od toga i u kojoj meri, ima li potrebe za odgovarajućom reakcijom Poverenika, itd.

Rezultati nadzora su nas iznenadili. Kao prvo, sva 4 operatera primili su nešto više od 4.000 zahteva za pristup zadržanim podacima, što nam se u prvom momentu učinilo vrlo malo. Sledeće što smo primetili, a što objašnjava zašto ima toliko malo zahteva, jeste da se istovremeno primenjuje samostalni pristup zadržanim podacima, znači službe bezbednosti su u prilici da samostalno, bez podnošenja zahteva za pristup zadržanim podacima, pristupe istim. Iznenadilo nas je što je oko 90 posto tih zahteva odobreno, a dodatno nas je iznenadilo što u velikom broju zahteva nije naveden pravni osnov po kom se traži pristup zadržanim podacima. Ipak, provajderi su po pravilu izlazili u susret svim zahtevima.

Nadalje, jedan provajder je obavestio Poverenika da je evidentirao nešto više od 270.000 samostalnih pristupa zadržanim podacima za period od godinu dana. Činjenica je da provajderi nemaju zakonsku obavezu evidentranja ovakvih pristupa, ali ta činjenica da je samo jedan operator evidentirao toliko ostvarenih samostalnih pristupa ukazuje da su i ostali operatori imali verovatno sličan broj ostvarenih samostalnih pristupa. Na osnovu toga možemo da zaključimo da ukupno (uzimajući u obzir sva 4 provajdera u Srbiji) imamo oko nekoliko stotina hiljada, možda čak i milion samostalnih pristupa zadržanim podacima o ostvarenim komunikacijama građana. Ako taj podatak uporedimo sa oko 4.000 pristupa ostvarenih na osnovu upućenih zahteva, vidimo ogromnu disproporciju koja ukazuje da je samostalan pristup ovim podacima pravilo, a podnošenje zahteva izuzetak. Zato i ne čudi podatak da je od tih oko 4.000 zahteva bilo samo dva zahteva BIA i četiri VBA.

Kada analiziramo brojku od oko 270.000 samostalnih pristupa zadržanim podacima kod jednog operatera, trebalo bi da se upitamo da li je sve to bilo u skladu sa Ustavom, odnosno u svrhe vođenja krivičnog postupka ili zaštite bezbednosti države Srbije, ili je možda bilo zloupotreba samostalnih pristupa zadržanim podacima u privatne, komercijalne, političke ili kakve druge svrhe.

Ovakve sumnje u eventualne zloupotrebe eliminisalo bi sprovođenje u život ovih 14 mera Poverenika i Zaštitnika građana.

Poverenik je često, nakon objavljenih tih 14 mera, dobijao pitanje zašto nije preduzeo mere iz svoje nadležnosti, odnosno zašto nije npr. naredio otklanjanje nepravilnosti u određenom roku, ili privremeno zabranio ovakvu obradu podataka ili naredio brisanje podataka koji su prikupljeni bez pravnog osnova. Razlog tome je što su rezultati nadzora ukazali da su problemi sistemskog karaktera, za čije rešavanje je potrebno preduzeti iste takve, sistemske mere, a to su značajne izmene postojećih zakona (posebno ZKP), donošenje nekoliko novih zakona, ujedinjavanje sada paralelno postojećih tehničkih mogućnosti službi bezbednosti i Policije u jednu nacionalnu agenciju za pružanje tehničkih usluga za pristup zadržanim podacima, ujedinjavanje procedura prema pružaocima elektronskih komunikacija, i dr. Dakle, radi se o sistemskim merama koje može i mora da preduzme država.

Danas je već bilo govora o odlukama Ustavnog suda o Zakonu o elektronskim komunikacijama i Zakonu o VBA i VOA. Ustavni sud je ocenio da pojedine odredbe ovih zakona nisu u saglasnosti sa Ustavom Srbije, jer je neko drugi, a ne isključivo sud, mogao da odluči da se odstupi od nepovredivosti tajnosti pisama i drugih sredstava komuniciranja.

Opšteprihvaćena pravila međunarodnog prava, a posebno praksa Evropskog suda za ljudska prava u Strasburu, kao i dosadašnja praksa Ustavnog suda, ukazuju nam da

zadržani podaci predstavljaju integralni element komunikacije, odnosno da se protivpravni pristup zadržanim podacima izjednačava protivpravnom pristupu samoj sadržini ostvarene komunikacije.

Ustavni sud se nije oglasio skoro 2 godine o predlogu Poverenika i Zaštitnika građana za ocenu ustavnosti Zakonika o krivičnom postupku, što u odnosu na period od 10 godina za ocenu ustavnosti Zakona o BIA i nije tako dug period.

Sad su pred nama dve osnovne mogućnosti postupanja dok čekamo na odluku Ustavnog suda o oceni ustavnosti odredbi ZKP, iako se na osnovu dosadašnje prakse ovog suda očigledno radi o nestavnim odredbama – prvo, istražiti tehnološke potencijale, savremena informatičarska i druga rešenja koja omogućavaju efikasno delovanje službi bezbednosti i Policije, te predmetnu oblast zakonski urediti u skladu sa realnim potrebama rada i Ustavom; i, drugo, ne činiti ništa dok Ustavni sud ne donese odluku, a onda ćemo da vidimo šta ćemo dalje. Ovaj drugi način sigurno nije doprinos efikasnom načinu rada službi bezbednosti i Policije, niti poštovanju ljudskih prava, posebno prava na privatnost.

I sasavim kratko, osvrnuću se još i na potrebu donošenja Zakona o bezbednosnim proverama, s obzirom da je upravo Poverenik inicirao donošenje ovog zakona. Razlog te inicijative je što je predmetna materija rasuta u više propisa, posebno u sferi obrazovanja i zapošljavanja u policiji, vojsci i službama bezbednosti. Smatramo da bi zakonom, u osnovi na jedinstven i celovit način, trebalo dosledno urediti vršenje bezbednosnih provera, a posebno sledeća pitanja: definicija osnovnih pojmova, pre svega bezbednosne provere i bezbednosne smetnje; vrste bezbednosnih provera koje se vrše; koji podaci se proveravaju, ko to čini i u kojim situacijama; funkcije, položaji, odnosno ličnosti koji su subjekti provera; svrha vršenja bezbednosnih provera; postupak vršenja bezbednosnih provera; rokovi vršenja bezbednosnih provera; posledice izvršenih bezbednosnih provera; način i rokovi čuvanja rezultata izvršenih bezbednosnih provera, kao i po potrebi druga pitanja koja bi definisali predstavnici nadležnih ministarstava, odnosno organa.

Nažalost, od inicijative Poverenika je proteklo dosta vremena, a po istoj, koliko mi je poznato, ništa nije preduzeto. Nadam se da će nova Vlada preduzeti odgovarajuće mere u tom cilju, a možda bi i danas najavljeni novi projekat CEAS mogao tome da doprinese.

Sanja Dašić, predstavnik Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka

Komentari i sugestije u vezi sa "Akcionim planom u 14 tačaka"

U vezi sa Nacrtom CEASovog Akcionog plana javnog zagovaranja usvajanja 14 tačaka Ombudsmana i Poverenika u okviru projekta "Promocija sveobuhvatne reforme sektora bezbednosti", Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka (*u daljem tekstu : KSNBiZTP*), kao nadležni organ u oblasti zaštite tajnih podataka u R. Srbiji, shodno nadležnostima iz Zakona o tajnosti podataka (članovi 86. i 87 stav 1 tačke od 1 do 12 Zakona), ima mandat da komentariše isključivo podatke iz svoje nadležnosti, a u konkretnom slučaju samo deo Akcionog plana koji se odnosi na navedeni Zakon.

Imajući u vidu da sastavni deo Vašeg Plana čini i 14 tačaka/preporuka, koje su još u julu 2012 . godine predložili Ombudsman i Poverenik, u okviru kojih se u tački 11 predlaže "preispitivanje rezultata sprovođenja Zakona o tajnosti podataka (uključujući usvajanje neophodnih podzakonskih akata, deklasifikaciju starih dokumenata, sprovođenje istraga, izdavanje bezbednosnih sertifikata...) i preduzimanje ozbiljnih izmena tog zakona ili donošenje novog smatramo celishodnim da Vam ukažemo da bi ovu tačku trebalo ažurirati imajući u vidu da Zakon ne tretira deklasifikaciju starih dokumenata i sprovođenje istraga. Naime, to je problematika u vezi sa drugim posebnim propisima koji se bave arhivskom građom ili pak sudskim postupcima.

Takođe, napominjemo da je u proteklom periodu došlo do određenih pomaka na planu donošenja podzakonskih akata koji bliže uređuju ovu oblast. Stupila je na snagu Uredba o bližim kriterijumima za određivanje dokumentata stepena tajnosti "državna tajna" i "strogo poverljivo", dok je u postupku donošenje Uredba o bližim kriterijumima za određivanje dokumentata stepena tajnosti "poverljivo" i "interno" za najveći broj organa javne vlasti, kao i Zakona o tzv. Informacionoj bezbednosti koji bi normativno trebalo da zaokruži oblast zaštite tajnih podataka na nacionalnom nivou. Ukazujemo i da je u toku formiranje Radne grupe za izmene i dopune Zakona o tajnosti podataka, koja ima za cilj otklanjanje uočenih manjkavosti i pravnih praznina postojećeg Zakona, kao i stvaranje uslova za efikasniju primenu samog Zakona.

Smatramo i da bi u tački 12 Akcionog plana umesto "poverljivi podaci" trebalo da stoji "tajni podaci", budući da je Poverljivo oznaka tajnosti a ne vrsta podatka .

O KSNBiZTP i njenim nadležnostima

KSNBiZTP predstavlja stručnu službu Vlade Republike Srbije, koja je formirana 16. novembra 2009. godine. U skladu sa Zakonom o osnovama uređenja službi bezbednosti ("Službeni glasnik RS", broj 116/07), KSNBiZTP vrši samo stručnu i *administrativnu podršku rada Saveta za nacionalnu bezbednost i Biroa za koordinaciju rada službi bezbednosti. Jedna od njenih nadležnosti odnosi se i na sprovođenje i kontrolu primene Zakona o tajnosti podataka* ("Službeni glasnik RS", broj 104/09), *kao i na aktivnosti u skladu sa propisima o državnoj upravi.*

U vezi sa sprovođenjem i kontrolom primene Zakona o tajnosti podataka, KSNBiZTP sprovodi *aktivnosti u vezi sa: primenom Zakona i donošenjem podzakonskih akata, međunarodnom saradnjom na planu razmene i zaštite tajnih podataka, izdavanjem sertifikata za pristup tajnim podacima i usavršavanjem državnih službenika iz organa državne uprave i službi Vlade.*

Inače, u skladu sa potpisanim i ratifikovanim međunarodnim sporazumima Kancelarija Saveta predstavlja *Nacionalni bezbednosni organ (NSA)* Republike Srbije. Naime, međunarodnu saradnju u oblasti razmene i zaštite tajnih podataka naša zemlja započela je zaključivanjem *Sporazuma između Vlade Republike Srbije i Organizacije severnoatlantskog pakta (NATO) o bezbednosti informacija i kodeksa o postupanju* ("Službeni glasnik RS - Međunarodni ugovori" 6/11) i zaključivanjem *Sporazuma između Republike Srbije i Evropske unije o bezbednosnim procedurama za razmenu i zaštitu tajnih podataka* ("Službeni glasnik RS - Međunarodni ugovori", br 1/2012.).

Za potrebe primene ovih sporazuma formiran je Centralni registar za strane tajne podatke u Kancelariji Saveta, kao i podregistri u Ministarstvu spoljnih poslova, Misiji Republike Srbije pri NATO i Misiji Republike Srbije pri Evropskoj uniji u Briselu, Ministarstvu unutrašnjih poslova, Ministarstvu odbrane i Bezbednosno-informativnoj agenciji. Sa razmenom tajnih podataka sa NATO i EU, otpočelo se nakon formiranja Centralnog registara i navedenih podregistara, kao i izvršenom sertifikacionom posetom ekspertskog tima NATO, a zatim i Evropske unije.

Pored toga, potpisano je još sedam sporazuma o razmeni i zaštiti tajnih podataka i to sa, *Slovačkom, Bugarskom, Češkom, Slovenijom, Bosnom i Hercegovinom, Makedonijom i Španijom*, dok su sa određenim državama inicirane aktivnosti na ovom planu i nalaze se u različitim fazama realizacije.

O CENTRU ZA EVROATLANTSKE STUDIJE (CEAS)

Centar za evroatlantske studije – CEAS je nezavisni, ateistički, socio-liberalno orijentisan, istraživački think-tank, koji se void ideologijom i vrednostima, a ne članstvom. Osnovan je 2007. godine u Beogradu od strane veoma male grupe istomišljenika na osnovu njihovih zajedničkih, gorenavedenih vrednosti i zajedničkog interesa u vezi sa globalnim i regionalnim trendovima, spoljnopolitičke orijentacije zemlje, reforme sektora bezbednosti i odbrane i tranzicione pravde u Srbiji. Ispostavilo se da je postojala realna potreba za takvom organizacijom u Srbiji i da je CEAS ispunion to potrebu.

U svim svojim aktivnostima CEAS stremi ka tome da obrazuje ili savetuje kreatore politike i javnost promovišući inovativne, primenljive i praktične politike čiji je cilj:

- Praćenje trendova i razvoja u socio-liberalnim studijama i prakse, i jačanje socio-liberalne demokratije u Srbiji;
- Usvajanje principa primate individualnih nad kolektivnim pravima, ne zanemarujući prava koja pojedinci mogu da ostvare samo u zajednici sa drugima;
- Jačanje principa sekularne države i promocija ateističkog pogleda na svet;
- Doprinos izgradnji i očuvanju otvorenijeg, bezbednijeg, prosperitetnijeg i kooperativnijeg svetskog poretka, zasnovanog na principima pametne globalizacije i ravnomernog održivog razvoja.

Svojim visoko-kvalitetnim istraživanjem i radom, CEAS generiše precizne i snažno priznate analize, uglavnom u polju spoljne, bezbednosne i odbrambene politike Republike Srbije, sa posebnim fokusom na:

- Ubrzavanje procesa EU integracije Srbije i jačanje njenih kapaciteta za suočavanje sa globalnim izazovima kroz zajedničko međunarodno delovanje, što void do punog i aktivnog članstva Srbije u EU;
- Jačanje saradnje sa NATO i zagovaranje punog i aktivnog članstva Srbije u Alijansi;
- Promociju važnosti regionalne saradnje;
- Nametanje robusne arhitekture demokratskog nadzora na sistemom bezbednosti;
- Podršku razvoja mehanizama tranzicione pravde, njihove promene u Srbiji i na Zapadnom Balkanu i razmena pozitivnih iskustava; naglašavanje važnosti mehanizama tranzicione pravde za uspešnu reform sektora bezbednosti u post-konfliktnim društvima na putu ka demokratiji.

CEAS je prva organizacija civilnog društva iz regiona jugoistočne Evrope sa punim članstvom u Međunarodnoj Koaliciji za Odgovornost da se zaštiti - ICRtoP. Koalicija okuplja nevladine organizacije iz svih delova sveta radi zajedničkog delovanja na jačanju normativnog konsenzusa oko doktrine odgovornosti da se zaštiti (Responsibility to Protect, skraćeno RtoP), u cilju boljeg razumevanja norme, pritiska na jačanju kapaciteta međunarodne zajednice da spreči ili zaustavi zločine genocida, ratne zločine, etničko čišćenje i zločine protiv čovečnosti i mobilizacije nevladinog sektora za zalaganje za akcije spasavanja ljudskih života u situacijama gde je primenjiva doktrina RtoP.

CEAS je takođe član Asocijacije za otvoreno društvo – PASOS, međunarodne asocijacije ekspertskih nevladinih organizacija (think-tanks) iz Evrope i Centralne Azije koja podržava izgradnju i funkcionisanje otvorenog društva, naročito u vezi sa pitanjima političke i ekonomske tranzicije, demokratizacije i ljudskih prava, otvaranja privrede i dobrog javnog upravljanja, održivog razvoja i međunarodne saradnje.

CEAS je prva organizacija civilnog društva u Srbiji koja je pristupila Komisiji Udruženja Privredne komore Srbije za javno-privatno partnerstvo u sektoru bezbednosti u Srbiji. Pored predstavnika privatnog sektora bezbednosti Komisija se takođe sastoji od predstavnika Ministarstva unutrašnjih poslova Srbije i drugih državnih organa i institucija koje su u toku obavljanja svojih dužnosti državne uprave nadležne za saradnju između javnog i privatnog sektora bezbednosti .

Osim toga, CEAS je i član Sektorkih organizacija civilnog društva - SEKO, u sektoru za vladavinu prava. Programom Kancelarije Vlade Srbije za evropske integracije i saradnju sa organizacijama civilnog društva u pogledu planiranja razvojne pomoći, posebno programiranja i praćenja korišćenja Instrumenta za pretpristupnu pomoć za 2011. Predviđeno je formiranje konsultativnog mehanizma sa OCD koji predviđa sektorske organizacije civilnog društva (SEKO) kao glavne nosioce aktivnosti .

CEAS i njegov tim članovi su Atlantske zajednice, prvog onlajn think tanka koji se bavi spoljnom politikom, prvenstveno fokusiran na pitanja koja se tiču transatlantskih odnosa, sa brojnim posebnim izdanjima, odeljcima i događajima koji promovišu debatu i zajednička rešenja za transatlantska pitanja i daju članovima mogućnost pristupa kreatorima politike .

CEAS takođe ima status posmatrača u Koaliciji za REKOM koja se zalaže da vlade (ili države) uspostave REKOM, nezavisnu, međudržavnu Regionalnu komisiju za utvrđivanje činjenica o svim žrtvama ratnih zločina i drugim teškim kršenjima ljudskih prava koja su se desila na teritoriji bivše SFRJ u periodu 1991.- 2001.