PERSPEKTIVE IMPLEMENTACIJE EVROPSKIH STANDARDA U PRAVNI SISTEM SRBIJE

KNJIGA 3

ZBORNIK RADOVA

Priredio
Prof. dr Stevan Lilić

Beograd, 2013

Lektor i korektor
Irena Popović

Tehnički urednik
Zoran Grac

Korice
Marija Vuksanović

Priprema i štampa
Dosije studio, Beograd

ISBN 978-86-7630-431-8

Tiraž
500

Adresa redakcije
Pravni fakultet Univerziteta u Beogradu
Centar za izdavaštvo i informisanje
Bulevar kralja Aleksandra 67
Tel./faks: 30-27-725, 30-27-776
e-mail: centar@ius.bg.ac.rs
web: www.ius.bg.ac.rs

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

340.137(4-672EU:497.11)(082)

PERSPEKTIVE implementacije evropskih standarda u pravni sistem Srbije : zbornik radova. Knj. 3 / priredio Stevan Lilić. – Beograd : Pravni fakultet, Centar za izdavaštvo i informisanje, 2013 (Beograd : Dosije studio). – 361 str. ; 24 cm. - (Biblioteka Zbornici)

Na spor. nasl. str.: Perspectives of Implementation of European Standards in Serbian Legal System. – Tekst lat. i ćir. – Tiraž 500. – Str. 9–10: Predgovor / urednik ; Forward / editor. – Napomene i bibliografske reference uz tekst. – Summaries.

ISBN 978-86-7630-431-8

1. Лилић, Стеван [уредник] [аутор додатног текста]

а) Право – Хармонизација – Европска унија – Србија – Зборници

COBISS.SR-ID 203584268

*Doc. dr Mirjana Drenovak Ivanović**

PRAVO NA PRIVATNOST I UPOTREBA MERA ELEKTRONSKOG NADZORA INFORMACIONIH SISTEMA

Apstrakt

U junu 2013. godine Evropski sud za ljudska prava doneo je presudu u vezi sa pravom na pristup informacijama o upotrebi mera elektronskog nadzora informacionih sistema u slučaju protiv Srbije. U stručnoj javnosti su tim povodom otvorena brojna pitanja: koji su uslovi za prikupljanje i obradu podataka o ličnosti; na koji način se informacije mogu zadržati i ko ima pravo na pristup zadržanim informacijama; ko i pod kojim uslovima ima pravo da vrši elektronski nadzor informacionih sistema; kakav je odnos između prikupljanja podataka i informacije o prikupljenim podacima; pod kojim uslovima se može pristupiti informacijama o ostvarenoj komunikaciji. U radu se analizira geneza postojećih zakonskih rešenja i ukazuje na Odluku Ustavnog suda Srbije o utvrđivanju nesaglasnosti Zakona o zaštiti podataka o ličnosti sa Ustavom (IУз–41/2010 od 30. maja 2012. godine), Odluku Ustavnog suda Srbije o utvrđivanju nesaglasnosti Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji sa Ustavom (IУз–1218/2010, od 19. aprila 2012. godine), Odluku Ustavnog suda Srbije o utvrđivanju nesaglasnosti Zakona o elektronskim komunikacijama sa Ustavom (IУз–1245/2010, od 8. jula 2013. godine).

Ključne reči: *Presretanje elektronskih komunikacija. Pravni osnov za obradu podataka o ličnosti. Praksa Ustavnog suda Srbije. Član 8 EKLJP.*

1. Uvod

Svaki podatak koji se odnosi na fizičko lice i koji to lice određuje ili čini odredivim jeste podatak o ličnosti.[1] Zaštita podataka o ličnosti zagarantovana je i Ustavom.[2] Upotreba podataka o ličnosti osim u svrhu za koju su prikupljeni nije dozvoljena. Izuzetno, podaci o ličnosti se mogu koristiti i izvan

* Dr Mirjana Drenovak Ivanović, docent Pravnog fakulteta Univerziteta u Beogradu. Rad je rezultat istraživanja u okviru projekta *Perspektive implementacije evropskih standarda u pravni sistem Srbije* (179059), koji podržava Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije.

1 Na ovaj način je podatak o ličnosti određen u Zakonu o zaštiti podataka o ličnosti. U uporednoj teoriji ne nailazimo na jedinstven stav o pojmu podataka o ličnosti. Vid. Maritxell Fernández-Barrera, Giovanni Sartor, „System vs. Computational Ontologies", Giovanni Sartor *et al.* (ur.), *Approaches to Legal Ontologies: Theories, Domains, Methodologies*, Springer, 2010, str. 18–20. i Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-Operation*, Martinus Nijhoff Publishers, 2008, 140–141.

2 *Ustav Republike Srbije*, „Službeni glasnik RS", br. 98/06, čl. 42.

svrhe za koju su prikupljeni ako je to neophodno za vođenje krivičnog postupka ili zaštitu nacionalne bezbednosti. Kako bi se zaštitili podaci o ličnosti i pravo na privatnost lica na koje se podaci odnose, prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuju se posebnim zakonom.

Zaštita podataka o ličnosti je na teritoriji Srbije prvi put normirana donošenjem Zakona o potvrđivanju Konvencije o automatskoj obradi ličnih podataka.[3] Nakon toga, usvojen je i Zakon o zaštiti podataka o ličnosti.[4] Tokom 2008. godine donet je Zakon o zaštiti podataka o ličnosti (dalje: ZZPL) koji sadrži nove standarde zaštite prava na privatnost.[5] Tim zakonom, poverenik za informacije od javnog značaja je dobio posebnu ulogu u zaštiti podataka o ličnosti, čime je postao i poverenik za zaštitu podataka o ličnosti.

Podaci o ličnosti se, po pravilu, prikupljaju i obrađuju samo uz pristanak lica na koje se odnose. Pojava savremenih bezbednosnih pretnji poput terorizma, organizovanog kriminala, korupcije i novih oblika ugrožavanja nacionalne bezbednosti dovode do potrebe proširenja upotrebe podataka o ličnosti. Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda u članu 8 utvrđuje da svako ima pravo na poštovanje svog privatnog i porodičnog doma i prepiske. Međutim, javne vlasti se mogu umešati u vršenje tog prava ako je to „u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda i kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih".[6] Jedan od načina pristupa podacima o ličnosti jeste i pristup zadržanim podacima. Kako se normiranjem pristupa zadržanim podacima ne bi izašlo iz okvira prava na poštovanje privatnog i porodičnog doma i prepiske, svaki novi instrument koji omogućava takve aktivnosti mora da bude usklađen sa Evropskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda.[7]

U radu se ukazuje na genezu pozitivnog zakonskog okvira kojim je uređeno pravo na pristup podacima o ličnosti. U radu se, dalje, pronalaze odgovori na pitanja koji su uslovi za prikupljanje i obradu podataka o ličnosti; na koji način se informacije mogu zadržati i ko ima pravo na pristup zadržanim informacijama; ko i pod kojim uslovima ima pravo da vrši elektronski nadzor informacionih sistema; pod kojim uslovima se može pristupiti informacijama o ostvarenoj komunikaciji. U radu se analiziraju postojeća zakonska rešenja i ukazuje na ulogu prakse Ustavnog suda Srbije u njihovoj transformaciji.

3 *Zakon o potvrđivanju Konvencije o automatskoj obradi ličnih podataka*, „Službeni list SRJ", br. Međunarodni ugovori, 1/92.

4 *Zakona o zaštiti podataka o ličnosti*, „Službeni list SRJ – Međunarodni ugovori", br. 24/98 i 26/98.

5 *Zakon o zaštiti podataka o ličnosti*, „Službeni glasnik RS", br. 97/2008, 104/2009, 68/2012 – Odluka Ustavnog suda.

6 *Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda*, „Službeni list Srbije i Crne Gore – Međunarodni ugovori", br. 9/03, čl. 8 st. 2.

7 Vid. *Directive 2004/24/EC of the European Partliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*, OJ [2006] L 105/54, Preambula recital 9.

2. Pojam zadržanih informacija

Radi sprovođenja neophodnih mera u borbi protiv terorizma, Evropski savet je u Deklaraciji o borbi protiv terorizma ukazao na potrebu utvrđivanja pravila o zadržavanju podataka o komunikacijskom saobraćaju od pružalaca usluga.[8] Definisanje pojma zadržanih podataka i pravila za zadržavanje i korišćenje tako prikupljenih podataka vode uspostavljanju garancija za poštovanje ljudskih prava, osnovnih sloboda i vladavine prava. Da bi se uspostavila zajednička pravila za zadržavanje podataka na evropskom nivou, 2006. godine doneta je Direktiva 2006/24/EZ Evropskog parlamenta i Saveta o zadržavanju generisanih ili obrađenih podataka u vezi sa odredbom u javnosti raspoloživih elektronskih komunikacionih servisa ili javne komunikacione mreže.[9] Direktivom normirana pravila odnose se na prikupljanje i obradu podataka u vezi sa komunikacijom, a ne na podatke koji predstavljaju sadržaj saopštene informacije. U skladu sa tim, pružaoci javno dostupnih usluga elektronskih komunikacija i javnih komunikacionih mreža imaju obavezu da zadrže određene kategorije podataka koji su nastali ili su obrađeni sa njihove strane. Prvoj kategoriji pripadaju podaci neophodni za praćenje i identifikaciju izvora neke komunikacije. Reč je o podacima koji su nastali u vezi sa korišćenjem usluga fiksne ili mobilne telefonije (pozivni telefonski broj ili ime i adresa korisnika) i podacima nastalim pristupom internetu, korišćenjem e-pošte ili internet telefonije. Drugoj kategoriji pripadaju podaci neophodni za identifikaciju odredišta neke komunikacije. Reč je o podacima o pozvanim brojevima, prosleđenim pozivima ili podacima koji omogućavaju identifikaciju lica kojima je e-pošta upućena. Trećoj kategoriji pripadaju podaci na osnovu kojih se mogu identifikovati datum, vreme i trajanje neke komunikacije, a četvrtoj podaci na osnovu kojih se može identifikovati vrsta komunikacije. Pružaoci javno dostupnih usluga elektronskih komunikacija i javnih komunikacionih mreža imaju obavezu da zadrže podatke o korisničkoj opremi za komunikaciju, kao i podatke neophodne za identifikaciju lokacije opreme mobilne komunikacije.[10]

U našem pravu, mogućnost zadržavanja podataka uređena je Zakonom o elektronskim komunikacijama.[11] Operator javnih komunikacionih mreža ili operator javno dostupnih elektronskih komunikacionih usluga ima obavezu da, od trenutka kada podaci o saobraćaju više nisu neophodni za prenos komunikacije, te podatke obriše ili izmeni informacije koje omogućavaju identifikaciju lica na koja se podaci o saobraćaju odnose. Međutim, zakon određuje i izuzetak koji se odnosi na obavezu zadržavanja podataka koji se primenjuje samo u zakonom propisanim okvirima.[12]

8 *Declaration on Combating Terrorism*, OJ [2005] C 14.

9 *Directive 2004/24/EC of the European Partliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*, OJ [2006] L 105/54.

10 *Direktiva 2004/24/EC*, član 5.

11 *Zakon o elektronskim komunikacijama*, „Službeni glasnik RS", br. 44/10 i 60/13 – Odluka Ustavnog suda.

12 *Ibid.*, čl. 122 st. 1.

3. Subjekti ovlašćeni na vršenje elektronskog nadzora informacionih sistema

U obavljanju dužnosti, Vojnobezbednosna agencija (VBA) ovlašćena je da prikuplja podatke od fizičkih lica. Zakonom o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji (dalje: Zakon o VBA) uređeno je da se prikupljanje podataka može izvršiti samo uz prethodni pristanak lica na koje se podaci odnose.[13] Ako se podaci ne mogu prikupiti od fizičkih lica, uz njihov prethodni pristanak, ili ako prikupljanje informacija „prouzrokuje nesrazmeran rizik po život i zdravlje ljudi i imovinu", VBA može primeniti posebne postupke i mere tajnog prikupljanja podataka.[14]

Jedan od postupaka tajnog prikupljanja podataka obuhvata „tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju, bez uvida u njihov sadržaj".[15] Posebni postupci i mere prikupljanja podataka primenjuju se „prevashodno u preventivne svrhe, odnosno sa ciljem da se preduprede pretnje koje su usmerene prema Ministarstvu odbrane i Vojsci Srbije".[16] Time se otvara pitanje ko je nadležan za donošenje odluke o sprovođenju ove posedne mere.

Prema Zakonu o VBA iz 2009. godine, tajni elektronski nadzor telekomunikacija i informacionih sistema preduzima se na osnovu naloga direktora VBA ili lica koje on ovlasti, a o izdatim nalazima se vodi evidencija.[17] Tajnim elektronskim nadzorom mogu se prikupiti informacije o korisnicima usluga operatora, obavljenoj komunikaciji, lokaciji sa koje se obavlja komunikacija, ali i „drugi podaci od značaja za rezultate primene posebnih postupaka i mera".[18] Tim povodom, otvoreno je pitanje da li VBA ima pravo da od telekomunikacionih operatera zahteva pristup zadržanim podacima, bez odluke suda, imajući u vidu da se time odstupa od Ustavom normirane nepovredivosti tajnosti pisama i drugih sredstava komuniciranja. Ustavni sud je u postupku po zajedničkom Predlogu zaštitnika građana i poverenika za informacije od javnog značaja o utvrđivanju saglasnosti Zakona o VBA sa Ustavom doneo Odluku u kojoj se, između ostalog, navodi:

> „Ustavni sud je, polazeći od odredaba člana 41. stav 2. Ustava koje propisuju da je odstupanje od nepovredivosti tajnosti pisama i drugih sredstava komuniciranja moguće samo na osnovu odluke suda, utvrdio da je jedino sud nadležan da, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na određeno vreme i na način predviđen zakonom, odredi (dozvoli) odstupanje od

13 *Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji*, „Službeni glasnik RS", br. 88/09, 55/12 – odluka Ustavnog suda i 17/13, čl. 8 st. 1.

14 *Ibid.*, čl. 10 i čl. 11.

15 *Ibid.*, čl. 12 st. 1 tač. 5.

16 *Ibid.*, čl. 11 st. 2.

17 *Ibid.*, čl. 13.

18 *Ibid.*, čl. 16 st. 2.

Ustavom zajemčene nepovredivosti tajnosti pisama i drugih sredstava komuniciranja. Kako iz osporene odredbe člana 13. stav 1. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, kojom je propisano da se posebni postupci i mere tajnog prikupljanja podataka iz člana 12. tačka 6) Zakona (tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja podataka o telekomunikacionom saobraćaju i lokaciji korisnika, bez uvida u njihov sadržaj) preduzimaju samo na osnovu naloga direktora Vojnobezbednosne agencije ili lica koje on ovlasti, to očigledno sledi da je osporenim zakonskim odredbama dozvoljeno odstupanje od zajemčene nepovredivosti tajnosti sredstava komuniciranja i bez odluke suda. Iz navedenog, po oceni Suda, proizlazi da propisane mere tajnog elektronskog nadzora telekomunikacija i informacionih sistema radi prikupljanja podataka o telekomunikacionom saobraćaju i lokaciji korisnika, čak i bez uvida u njihov sadržaj, narušavaju nepovredivost prava na privatnost prepiske, odnosno tajnosti sredstava komuniciranja korisnika komunikacionih mreža, s obzirom na to da nadležne službe bezbednosti te mere mogu vršiti bez prethodno pribavljene odluke suda, koja upravo treba da predstavlja oblik kontrole i neophodnu branu svakoj mogućoj zloupotrebi ovlašćenja od strane upravnih vlasti, zbog čega osporena odredba Zakona nije u saglasnosti sa Ustavom. (...) Ustavni sud nalazi da Vojnobezbednosna agencija, kao organ uprave, bez odgovarajuće odluke suda, nema sopstveno pravo na dobijanje informacija od telekomunikacionih operatora o korisnicima njihovih usluga o obavljenoj komunikaciji, lokaciji sa koje se obavlja i drugih podataka od značaja za rezultate primene posebnih postupaka i mera, jer i ti podaci predstavljaju integralni element zaštićene tajnosti komunikacije putem telefona, pa je, polazeći od navedenog, Ustavni sud ocenio da ni osporena odredba člana 16. stav 2. Zakona nije u saglasnosti sa članom 41. stav 2. Ustava."[19]

Nakon donošenja Odluke Ustavnog suda Srbije, donet je novi Zakon o VBA čija su rešenja usklađena sa Odlukom. Kako je reč o merama koje VBA treba da omoguće preduzimanje aktivnosti kojima se sprečava izvršenje opasnog delovanja terorista i ekstremista, ali kojima se u velikoj meri ograničava pravo na privatnost, njihovo preduzimanje je moguće samo na osnovu obrazložene odluke suda. Nadležnost je poverena višem sudu u sedištu apelacionog suda područja na kome se planira primena posebnih mera. Sudije koje će doneti odluku određuje predsednik višeg suda. O primeni posebnih mera sud odlučuje po hitnom postupku, tj. „bez odlaganja, a najkasnije u roku od osam sati".[20] Ako je neophodno hitno preduzimanje mera tajnog elektronskog nadzora telekomunikacija i informacionog sistema, direktor VBA može da naloži početak primene ovog postupka uz prethodnu saglasnost sudije,

19 *Odluka Ustavnog suda Srbije*, ИУз–1218/2010 od 19. aprila 2012. godine. Vid. i *Odluku Ustavnog suda Srbije*, ИУз–1245/2010, od 8. jula 2013. godine.

20 *Zakon o VBA*, čl. 13a st. 5.

koji je nadležan za donošenje odluke o primeni posebnih mera u redovnom postupku. O nastavku primene mere, sudija odlučuje u roku od 24 sata od početka primene.[21]

Tajni elektronski nadzor telekomunikacija i informacionih sistema, kao posebna mera, može se vršiti dok postoje razlozi za njeno sprovođenje, a najduže šest meseci. Međutim, sudija, čija se nadležnost utvrđuje kao pri donošenju odluke o primeni posebnih mera, može da produži njihovu primenu za još šest meseci. Kako je reč o posebnim merama, o produženju njihovog preduzimanja odlučuje Veće koje čini više sudija, uz preispitivanje rezultata do kojih se došlo primenom mera i opravdanosti produženja, čime se na bolji način izražava realizacija Ustavom garantovanog prava na zaštitu podataka o ličnosti i prava na tajnost pisama i drugih sredstava komunikacije.

Informacije sadržane u predlogu i odluci za sprovođenje tajnog elektronskog nadzora telekomunikacija i informacionih sistema, kao i informacije koje su službena lica saznala u postupku preduzimanja ovih mera predstavljaju tajnu. Pitanje koje se dalje otvara jeste na koji način je obezbeđena tajnost podataka po završetku sprovođenja posebnih mera. Prema ZZPL, prikupljeni podaci se moraju adekvatno zaštititi od zloupotreba i neovlašćenog pristupa.[22] Ipak, u Zakonu o VBA je normirano da na predlog VBA, po pribavljenom mišljenju Saveta za nacionalnu bezbednost, ministar odbrane uređuje način zaštite, rukovanja i rokove čuvanja zbirki podataka.[23] To dalje znači da se podaci prikupljeni u preventivne svrhe mogu čuvati i nakon prestanka potrebe koja je uslovila njihovo prikupljanje. Da bi se obezbedila bolja zaštita prikupljenih podataka, po prestanku potrebe za primenom posebnih mera, Zakonom o VBA bi trebalo da se postupanja sa tim podacima normira na drugačiji način u odnosu na postupanje sa ostalim podacima. Treba primeniti jasno pravilo poput onoga kojim se utvrđuje obaveza komisijskog uništavanja prikupljenih podataka uz dostavljanje sudu zapisnika o tome u slučaju ako nadležni sudija ne odobri primenu posebnih postupaka.[24] Ako odluku o primeni posebnih mera tajnog elektronskog nadzora telekomunikacija i informacionih sistema donosi sud, onda je i određivanje rokova u kojima će se tako prikupljene informacije čuvati pitanje o kojem sud treba da odluči. Postupak se može urediti tako da, po završenom sprovođenju posebnih mera, nadležni organ VBA dostavlja sudu, koji je doneo odluku o sprovođenju posebnih mera, zapisnik o završetku primene određenih mera, uz predlog o načinu na koji će se čuvati informacije prikupljene u preventivne svrhe i o rokovima. Uvođenje pravila da sud odlučuje o donošenju odluke a da nadležni organ VBA odlučuju o tome da li će se tajno prikupljene informacije čuvati i po prestanku potrebe za sprovođenje posebne mere, na koji način i u kojem roku, otvara mogućnost za nejednako postupanje koje može dovesti do povrede Ustavom garantovanih prava.

21 *Ibid.*, čl. 15.

22 *ZZPL*, čl. 47.

23 *Zakon o VBA*, čl. 32.

24 *Ibid.*, čl. 15 st. 3.

4. Normiranje postupka prikupljanja, držanja, obrade i korišćenja podataka

U skladu sa Ustavom, podaci o ličnosti se mogu upotrebiti „samo u svrhu za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom".[25] U ZZPL-u je kao nedozvoljena obrada podataka kvalifikovana ona za koju fizičko lice nije dalo pristanak ili koja se vrši bez zakonskog ovlašćenja.[26] Analiza Ustava Srbije (član 42) i ZZPL (član 8, član 12 i član 13) pokazuje da rukovalac informacijama može da prikuplja i obrađuje informacije o ličnosti za čije je prikupljanje ovlašćen zakonom ili one podatke za čije je prikupljanje i obradu dobio saglasnost lica na koje se odnose. Pri tome, rukovalac informacijama može da prikuplja informacije u zakonom propisanu svrhu ili u svrhu koja je određena dobijenim pristankom. Podaci o ličnosti se, izuzetno, mogu prikupljati „da bi se ostvarili ili zaštitili važni interesi lica, a posebno život, zdravlje i fizički integritet, u svrhu izvršenja obaveza određenih zakonom, aktom donetim u skladu sa zakonom; (...) u drugim slučajevima određenim zakonom radi ostvarenja pretežnog opravdanog interesa lica, rukovaoca ili korisnika podataka".[27]

U skladu sa ZZPL-om iz 2009. godine, organ vlasti je imao mogućnost da podatke obrađuje bez pristanka lica ako je to neophodno radi obavljanja zakonom ili drugim propisom određenih nadležnosti.[28] Osim toga, normirano je da se podaci o ličnosti mogu prikupljati od lica na koja se odnose, organa uprave koji su ovlašćeni za njihovo prikupljanje, kao i drugih lica „ako je to propisano zakonom ili drugim propisom donetim u skladu sa zakonom".[29] Ta rešenja su otvorila sledeća pitanja: da li osnov za obradu podataka o ličnosti može da bude samo zakon ili i akt niže pravne snage? Da li treba podrazumevati da akt niže pravne snage koji propisuje obradu podataka o ličnosti bez pristanka lica na koje se odnosi mora da bude u skladu sa ZZPL-om? Da li se aktom niže pravne snage može odrediti nadležnost za obavljanje poslova koje se odnosi i na obradu podataka bez pristanka lica od strane organa vlasti?

Ustavni sud Srbije je, na predlog poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti za ocenu ustavnosti odredaba ZZPL-a iz 2009. godine, doneo odluku u kojoj se, između ostalog, navodi:

> „Kako se Zakonom o zaštiti podataka o ličnosti daje mogućnost obrade podataka o ličnosti bez pristanka lica i u slučajevima određenim ovim zakonom ili drugim propisom donetim u skladu sa ovim zakonom, da organ vlasti obrađuje podatke bez pristanka lica, ako je obrada neophodna radi obavljanja poslova iz njegove nadležnosti određenih

25 *Ustav Republike Srbije*, čl. 42 st. 3.

26 *ZZPL*, čl. 8 st. 1 tač. 1.

27 *Ibid.*, čl. 12.

28 *Zakon o zaštiti podataka o ličnosti*, „Službeni glasnik RS", br. 97/2008, 104/2009, član 13.

29 *Ibid.*, čl. 14 st. 2 tač. 2

zakonom ili drugim propisom, kao i da se podaci mogu prikupljati i od drugog lica ako je to propisano zakonom ili drugim propisom donetim u skladu sa zakonom, to po oceni Suda, sledi da članovi Zakona u delu 'ili drugim propisom', odnosno 'ili drugim propisom donetim u skladu sa zakonom' nisu u saglasnosti sa članom 42. stav 2. i 3. Ustava, s obzirom na to da se tim odredbama Zakona predviđa da osnov za obradu podataka o ličnosti može, pored zakona, biti i akt niže pravne snage, odnosno podzakonski akt. (...) Ustavni sud je povodom odredbe člana 13. Zakona imao u vidu činjenicu da se reči 'ili drugim propisom' odnose na nadležnosti organa vlasti, te da pojedini poslovi iz nadležnosti tih organa mogu biti određeni ne samo zakonom već i drugim propisom (pre svega statutom i drugim opštim aktom autonomne pokrajine ili jedinice lokalne samouprave), ali, po oceni Suda, jedino je na osnovu zakona a ne na osnovu 'drugog propisa' moguće da organ vlasti, ako je to neophodno radi obavljanja poslova iz njegove nadležnosti, određene zakonom, obrađuje podatke bez pristanka lica."[30]

5. Pravo na obradu podataka prema Zakonu o elektronskim komunikacijama i Zakonu o telekomunikacijama

Moguća odstupanja od prikupljanja podataka o komunikaciji bez pristanka korisnika, normirana su i Zakonom o elektronskim komunikacijama. U slučaju kada je presretanje elektronske komunikacije neophodno radi vođenja krivičnog postupka ili zaštite nacionalne bezbednosti, operator je dužan da nadležnim organima omogući zakonito presretanje.[31] Operator ima obavezu da o svom trošku omogući tehničku opremu za presretanje elektronske komunikacije. U tom cilju, operator ima obavezu da podatke koji nastaju tokom obavljanja redovnih aktivnosti čuva 12 meseci, od dana obavljene komunikacije, u obliku koji omogućava brz pristup i dostavljanje.[32] Zadržani podaci se čuvaju od slučajnog ili nedopuštenog uništenja i neovlašćenog pristupa kao i ostali podaci o ličnosti.

Privatnost i bezbednost podataka uređene su i Zakonom o telekomunikacijama u skladu sa kojim je ustanovljena obaveza očuvanja bezbednosti i poverljivosti podataka nastalih u procesu redovne komunikacije, čiji je nosilac javni telekomunikacioni operator.[33] Operator ima pravo da čuva i obrađuje podatke o saobraćaju koji se odnose na tačno određene korisnike samo u obimu koji je neophodan za formiranje računa za naplatu u sluga, a takvi se podaci mogu čuvati samo do isteka roka u kome se potraživanje za obavljene

30 *Odluke Ustavnog suda Srbije*, IУз –41/2010 od 30. maja 2012. godine.

31 *Zakon o elektronskim komunikacijama*, čl. 127.

32 *Ibid.*, čl. 128.

33 *Zakon o telekomunikacijama*, „Službeni glasnik RS", br. 44/03, 36/06, 50/09 – odluka Ustavnog suda i 44/10, čl. 54.

usluge može od korisnika naplatiti ili osporiti. U Zakonu o telekomunikacijama iz 2009. godine normirana je zabrana sprovođenja aktivnosti kojima se narušava privatnost i poverljivost poruka koje se prenose telekomunikacionim mrežama. Istim Zakonom, normiran je i izuzetak koji se odnosi na mogućnost sprovođenja aktivnosti i korišćenja uređaja, uprkos mogućnosti da se time ugrozi privatnost podataka „ako se ove aktivnosti vrše u skladu sa zakonom ili sudskim nalogom izdatim u skladu sa zakonom".[34] U postupku ocene ustavnosti takvog rešenja Ustavni sud Srbije je izneo sledeće:

> „Prema odredbama člana 20. stav 1. i člana 41. stav 2. Ustava, samo je sud nadležan da, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike, na određeno vreme i na način predviđen zakonom odredi, odnosno dozvoli odstupanje od Ustavom zajemčene nepovredivosti tajnosti pisama i drugih sredstava komuniciranja. Kako je osporenom odredbom člana 55. stav 1. navedenog zakona bila propisana dozvoljenost odstupanja od zabrane aktivnosti ili korišćenja uređaja kojima se ugrožava ili narušava poverljivost poruka koje se prenose telekomunikacionim mrežama, ne samo kada se vrše u skladu sa sudskom odlukom, već i bez posebnog naloga suda, kada je takva mogućnost propisana tim ili drugim zakonom, Ustavni sud je ocenio da se aktivnosti ili korišćenje uređaja kojima se ugrožava ili narušava privatnost i poverljivost poruka ne mogu vršiti bez odluke suda, te da stoga osporena odredba, u delu koji glasi: 'zakonom ili', nije u saglasnosti sa Ustavom."[35]

6. Zaključak

Na osnovu prethodne analize i odgovora na postavljena pitanja možemo izvesti nekoliko zaključaka. Osnov zaštite podataka o ličnosti postavljen je Ustavom koji normira da je zagarantovana zaštita podataka o ličnosti i da se prikupljanje i postupanje sa tim podacima uređuju posebnim zakonom. Ustavom se, takođe, utvrđuje da upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni nije dozvoljena, uz izuzetak koji postoji kada je upotreba podataka neophodna za vođenje krivičnog postupka ili zaštitu nacionalne bezbednosti. U skladu sa Zakonom o zaštiti podataka o ličnosti, pravo da koristi prikupljene podatke ima organ vlasti, fizičko ili pravno lice koje je na to zakonom ovlašćeno ili koje je za postupanje u vezi sa podacima o ličnosti dobilo pristanak lica na koje se podaci odnose. To znači da pravni osnov za prikupljanje i obradu podataka o ličnosti predstavlja ili saglasnost lica na koja se odnose ili zakonsko ovlašćenje.

Pristup podacima o komunikaciji između lica, kao vrsta podatka o ličnosti, uređen je i Zakonom o elektronskim komunikacijama i Zakonom o telekomunikacijama. Pre donošenja analiziranih Odluka Ustavnog suda ti

34 *Zakon o telekomunikacijama*, „Službeni glasnik RS", br. 44/03 i 36/06, čl. 55 st.1.

35 *Odluka Ustavnog suda Srbije*, IУз –149/2008 od 28. maja 2009. godine.

zakoni, kao i Zakon o zaštiti podataka o ličnosti iz 2009. godine, normirali su mogućnost pristupa podacima o ličnosti bez pristanka lica na koje se odnose, na osnovu zakona, ali i podzakonskog akta. Ustavni sud je u obrazloženju Odluke o utvrđivanju nesaglasnosti Zakona o zaštiti podataka o ličnosti sa Ustavom (ИУз–41/2010 od 30. maja 2012. godine), Odluke o utvrđivanju nesaglasnosti Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji sa Ustavom (ИУз–1218/2010, od 19. aprila 2012. godine) i Odluke o utvrđivanju nesaglasnosti Zakona o elektronskim komunikacijama sa Ustavom (ИУз–1245/2010, od 8. jula 2013. godine), ukazao na važnost Ustavom garantovane zaštite podataka o ličnosti i tajnosti pisama i drugih sredstava komunikacije. Potreba zaštite Ustavom garantovanih vrednosti nalaže primenu izuzetaka koji mogu da budu normirani isključivo zakonom, a ne i aktom niže pravne snage. Imajući u vidu značaj odluka Ustavnog suda na izmene zakona koji uređuju pitanje zaštite podataka o ličnosti i poverljivosti komunikacije, zaključujemo da su poverenik za informacije od javnog značaja i zaštitu podatka o ličnosti, zaštitnik građana i praksa Ustavnog suda Srbije imali ključnu ulogu u razvoju zaštite podataka o ličnosti.

Dodatna pravna zaštita može se postići izmenama rešenja Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji koja se odnose na mogućnost čuvanja prikupljenih podataka i po prestanku potrebe za primenom posebnih mera. U skladu sa važećim rešenjima, o rokovima čuvanja podataka odlučuje nadležni organ VBA. Ako odluku o primeni posebnih mera tajnog elektronskog nadzora telekomunikacija i informacionih sistema donosi sud, onda je i određivanje rokova u kojima će se tako prikupljene informacije čuvati pitanje o kojem treba da odluči sud. Prema tome, novim zakonskim rešenjima trebalo bi definisati ulogu suda u donošenju odluke o načinu i rokovima za čuvanje prikupljenih podataka.

*Doc. dr. Mirjana Drenovak Ivanović**

THE RIGHT TO PRIVACY AND LAWFUL INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Summary

The European Court of Human Rights has recently delivered a judgement in the case of the right to access public information related to interception of electronic communications concerning the implementation of Article 10 of the Convention in Serbia. This judgement has opened a number of questions: under

* Mirjana Drenovak Ivanović, PhD. Assistant professor Faculty of Law University of Belgrade. This article is the result of research within the project *Perspectives of Implementation of European Standards in the Serbian Legal System* (179059), supported by the Ministry of Education, Science and Technological Development.

what conditions the personal data may be processing and collected; under what conditions interception of electronic communications is lawful; who has the authority to access to those information; who has the authority to demand the interception on electronic communications; what relation does it exist between the data collection and the information on it? The paper analyzes development of legal framework concerning the right to privacy and interception of electronics communications and points out the Decision of Serbian Constitutional Court on the Proposal to review the constitutionality of provisions of the Law on data protection (ИУз–41/2010, from May 30, 2012.), the Decision of Serbian Constitutional Court on the Proposal to review the constitutionality of provisions of the Law on Military Security Agency and Military Intelligence Agency (ИУз–1218/2010, from April 19, 2012), and the Decision of Serbian Constitutional Court on the Proposal to review the constitutionality of provisions of the Law on electronic communications (ИУз–1245/2010, from July 8, 2013).

Key words: *Interception of electronic communications. The legal grounds for data processing. Case law of the Serbian Constitution Court. Article 8 of the ECHR.*