Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji?

Ko nas prisluškuje?

Jelena Pejić

BCBP

KO NAS PRISLUŠKUJE?

Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim podacima u Srbiji?

Beograd, 2014.

KO NAS PRISLUŠKUJE?

Kako funkcioniše presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji?

IZDAVAČ
Beogradski centar za bezbednosnu politiku
Đure Jakšića 6/5, Beograd
Tel: 011 3287 226
Email: office@bezbednost.org
www.bezbednost.org

AUTORKA
Jelena Pejić

UREDNICA
Katarina Đokić

DIZAJN I PRELOM
Saša Đorđević

BEOGRAD, 2014.

Objavljivanje ovog rada podržala je Ambasada Kraljevine Norveške kroz projekat „Ko nas sluša: Ka efektivnom spoljnom nadzoru upotrebe specijalnih istražnih mera". Stavovi izneti u ovoj publikaciji predstavljaju stavove autorke i ne odražavaju nužno stavove Kraljevine Norveške.

POJMOVNIK

Naš svakodnevni život nezamisliv je bez telefona i interneta. Istovremeno, privatni razgovori mogu da budu predmet nadzora države. Cilj ovog teksta je da predoči javnosti u kojim okolnostima se to dešava.

ŠTA?

Nadzor nad elektronskim komunikacijama podrazumijeva dva tipa aktivnosti: zakonito presretanje komunikacija i pristup zadržanim elektronskim podacima. Suštinska razlika između njih jeste u tome što se jedino presretanjem ostvaruje uvid u sadržaj komunikacije. Laičkim rječnikom, presretanje znači prisluškivanje, ali nije vezano samo za pozive, nego i sms poruke, i-mejlove i ostale vrste elektronskog komuniciranja. Ono obuhvata mobilnu, fiksnu i internet telefoniju, elektronsku poštu i pristup internetu uopšte. S druge strane, zadržani podaci su bitni podaci o obavljenoj komunikaciji. To su: izvor i odredište komunikacije, vrijeme njenog početka, trajanja i završetka, vrsta komunikacije koja je obavljena, terminalna oprema korisnika i njegova lokacija.[1] Bez uvida u sadržaj komunikacije, operator je dužan sve to da zabilježi i uskladišti za narednih dvanaest mjeseci. Šta to znači u praksi? Uzmimo za primjer telefonski razgovor. To su podaci o tome koji broj je i koga zvao, kad i koliko dugo, kojim sredstvom i odakle, ali ne i o čemu su razgovarali. Sve ovo bilježi svaki operator za sve svoje korisnike, i to bez obzira da li je odgovoreno na poziv ili ne. Zadržavanje u stvari znači čuvanje na određeno vrijeme ogromnog broja podataka o svim komunikacijama, kako bi se u slučaju potrebe njima moglo naknadno pristupiti. Zakonom određen rok čuvanja je 12 mjeseci od dana kad je komunikacija obavljena.

[1] Zakon o elektronskim komunikacijama, čl. 129.

Posmatrajući širi pravni okvir, presretanje komunikacija i pristup zadržanim podacima spadaju u tzv. posebne mjere za tajno prikupljanje podataka. Primjena posebnih mjera, naime, znači zadiranje u neka osnovna građanska prava. U našem slučaju, to su nepovredivost tajnosti pisama i drugih sredstava opštenja, te zaštita podataka o ličnosti.[2] Ove mjere se u različitim zakonima „kriju" pod različitim imenima: posebne dokazne radnje, mjere ciljane potrage, posebni postupci i mjere tajnog prikupljanja podataka. U njih se ubraja i tajni nadzor komunikacija i informacionih sistema.[3]

PRAVNI OKVIR	NAZIV ZA POSEBNE MJERE	MJERE KOJE UKLJUČUJU PRESRETANJE LEKTRONSKIH KOMUNIKACIJA I PRISTUP ZADRŽANIM ELEKTRONSKIM PODACIMA
Zakonik o krivičnom postupku	Posebne dokazne radnje (čl. 161)	tajni nadzor komunikacija (čl. 166)
Zakon o VBA i VOA	Posebni postupci i mere tajnog prikupljanja podataka (čl. 10)	tajni nadzor sadržine pisama i drugih sredstava komuniciranja; tajni elektronski nadzor telekomunikacija i informacionih sistema radi prikupljanja zadržanih podataka o telekomunikacionom saobraćaju, bez uvida u njihov sadržaj (čl 12 – 7,5)
Zakon o BIA	Posebne mere kojima se odstupa od nepovredivosti tajne pisama i drugih sredstava opštenja (čl.13)	tajni nadzor i snimanje komunikacije; statistički elektronski nadzor komunikacije i informacionih sistema u cilju pribavlljanja podataka o komunikaciji ili lokaciji korišćene mobilne terminalne opreme; (čl. 13 – 1,3)
Zakon o policiji	Mere ciljane potrage (čl. 83)	Nisu posebno navedene

[2] Članovi 41 i 42 Ustava RS.

[3] V. ZKP čl. 161, ZBIA čl. 13, ZVBAiVOA čl.10 i ZP čl. 83.

KO?

Zakon o elektronskim komunikacijama kao predmetni zakon ne definiše precizno ko može da vrši zakonito presretanje poziva i pristupi zadržanim podacima. Umjesto toga nudi opštu formulaciju „nadležni organ". Ko su nadležni organi u ovom slučaju nalazimo u nekoliko drugih zakona. Zakon o krivičnom postupku je ovdje jasniji te, ubrajajući među posebne dokazne radnje i tajni nadzor komunikacije, određuje aktere koji mogu da ga sprovode: policija[4], Bezbednosno-informativna agencija (BIA) i Vojnobezbednosna agencija (VBA).[5] Njihova ovlašćenja potvrđena su i u pojedinačnim zakonima.[6]

Kao posebno ovlašćenje policije u predistražnom postupku izdvojeno je pribavljanje evidencije ostvarene telefonske komunikacije, korišćenih baznih stanica ili lociranje mjesta sa kojeg se obavlja komunikacija, a po nalogu koji sudija za prethodni postupak izdaje na prijedlog javnog tužioca.[7] Sve ovo spada u bitne podatke o komunikaciji, koje je operator u obavezi da zadrži.

ZAŠTO?

Postoje dva Ustavom propisana razloga za preduzimanje ovakvih specijalnih mjera. To su potrebe vođenja krivičnog postupka i zaštita bezbjednosti Republike Srbije.[8]

Kada je riječ o vođenju krivičnog postupka, objekat tajnog nadzora komunikacija može biti lice za koje postoje osnovi sumnje da je učinilo ili da priprema neko od težih krivičnih djela nabrojanih u Zakoniku o krivičnom postupku, ili ako sprečava ili ometa njihovo dokazivanje. U pitanju su, između ostalog, organizovani kriminal i ratni zločini, ubistvo i razbojništvo, dječija pornografija, trgovina narkoticima, oružjem i ljudima, napad na ustavno uređenje Republike Srbije, mito i korupcija. Tajni nadzor komunikacija se može primijeniti i za krivična djela neovlašćenog korišćenja autorskog djela, računarske prevare i sabotaže.[9] U ostalim slučajevima nema dovoljno jakog opravdanja za prodor u privatnu sferu građanina, tj. cilj ne bi mogao da opravda upotrijebljena sredstva.

---

4 U praksi je to Služba za specijalne istražne metode unutar Uprave kriminalističke policije.

5 ZKP, član 168.

6 V. članovi 30 i 83 ZP, član 13 Zakona o BIA (tek nakon izmjena i dopuna 2014. godine) i član 12 Zakona o VBA i VOA.

7 ZKP, član 286.

8 V. član 126, 128 ZEK, članovi 41 i 42 Ustava RS. Član 41 uređuje tajnost pisama i drugih sredstava opštenja, a član 42 uređuje zaštitu podataka. Oba spadaju u odredbe kojima se štiti privatnost građana.

9 ZKP, članovi 161-162.

Kada je u pitanju zaštita nacionalne bezbjednosti, BIA može primijeniti posebne mjere „prema licu, grupi ili organizaciji za koju postoje osnovi sumnje da preduzima ili priprema radnje usmerene protiv bezbednosti Republike Srbije (...)".[10] Krug djelovanja VBA je uži. Ova agencija primjenjuje posebne mjere u cilju predupređivanja prijetnji prema Ministarstvu odbrane i Vojsci Srbije, i to samo prema zaposlenima u ovim tijelima. Prema ostalim licima može ih primjenjivati samo uz saradnju sa policijom ili BIA.[11]

Svako ovlašćenje za primjenu specijalnih mjera mora, međutim, proći i sljedeće uslove:

1. neophodne podatke nije moguće prikupiti na drugi način, kojim se manje ograničavaju prava građana, ili bi njihovo prikupljanje bilo znatno otežano;
2. nepreduzimanje mjera bi moglo da izazove nesrazmjerne teškoće, troškove ili veliku opasnost. [12]

Specijalne mjere se, dakle, primjenjuju samo u krajnjem slučaju, kad je bilo kakvo drugačije postupanje nedjelotvorno i opasno.

KAKO?

Akteri koji vrše zakonito presretanje komunikacija i pristup zadržanim podacima ne mogu olako da ugrožavaju građanska prava. Osim propisanog razloga, potrebno je da ispoštuju zakonsku proceduru. Presretanje elektronskih komunikacija i pristup zadržanim podacima bez pristanka korisnika dopušteni su samo na određeno vrijeme i na osnovu odluke suda, ako postoji neki od prethodno razjašnjena dva razloga. Procedura se razlikuje u zavisnosti od toga koji razlog je u pitanju, procesuiranje krivičnih djela ili zaštita nacionalne bezbjednosti.

Kada je riječ o zaštiti nacionalne bezbjednosti, akteri predlažu sudu primjenu mjera. Ne može, međutim, bilo ko od zaposlenih u VBA, BIA ili policiji da se obrati bilo kojem sudu. Zakonski je uređeno ko je ovlašćeni predlagač i koji sud je nadležan za svakog od ovih aktera. Tako, u ime BIA prijedlog za primjenu specijalnih mjera upućuje direktor Agencije a odobrenje donosi predsjednik ili od njega ovlašćeni sudija Posebnog odeljenja (za organizovani kriminal) Višeg suda u Beogradu. Na osnovu prijedloga direktora VBA odluku o primjeni specijalnih mjera presretanja komunikacija donose ovlašćene sudije Vrhovnog kasacionog suda, a kada je riječ o pristupu zadržanim podacima odlučuje ovlašćeni sudija nadležnog višeg suda. Primjenu posebnih mjera od strane policije predlaže direktor policije, a odobrava je predsjednik ili od njega ovlašćeni sudija Vrhovnog kasacionog suda.

---

10 V. član 14 Zakona o BIA.

11 Član 23 Zakona o VBA i VOA.

12 V. čl. 161 ZKP, čl. 11 ZVBA i VOA, čl. 14 ZBIA, čl. 83 ZP.

Ukoliko je riječ o prikupljanju dokaza u krivičnom postupku, obrazloženi prijedlog daje javni tužilac, a naredbu o sprovođenju mjere donosi sudija za prethodni postupak.[13]

PRAVNI OKVIR	PREDLAGAČ	NADLEŽNI SUDIJA
Zakon o BIA	Direktor BIA	Predsjednik ili ovlašćeni sudija Višeg suda u Beogradu
Zakon o VBA i VOA	Direktor VBA	Ovlašćeni sudija Vrhovnog kasacionog suda (za presretanje komunikacija); ovlašćeni sudija nadležnog višeg suda (za pristup zadržanim podacima)
Zakon o policiji	Direktor policije	Predsjednik ili ovlašćeni sudija Vrhovnog kasacionog suda
Zakonik o krivičnom postupku	Javni tužilac	Sudija za prethodni postupak

Samo u slučaju hitnosti ili naknadnog proširenja specijalnih mjera, akteri prvo počinju sa njihovom primjenom pa tek naknadno dobijaju odobrenje nadležnog suda. Ukoliko ga ne dobiju, dužni su da sav prikupljeni materijal unište kao da mjeru nisu ni primjenjivali, odnosno proširivali.[14]

---

13 V. Član 13a ZVBA i VOA, član 15 ZBIA, član 83 ZP, član 167 ZKP.

14 V. član 169(3) ZKP, član 15b ZBIA, član 15 ZVBA i VOA.

ŠTA JE NEJASNO?

Nekoliko nejasnoća u vezi sa zakonitim presretanjem komunikacija i pristupom zadržanim elektronskim podacima proističe iz nepostojanja podzakonskog akta koji bi detaljno opisao procedure i definisao tehničke uslove za sprovođenje ovih radnji. Prijedlog takvog akta sastavljen je 2013. godine, ali još uvijek nije usvojen.[15]

Glavni problem je način na koji se utvrđuje ovlašćeno lice kod operatera koje je zaduženo da postupa po zahtevu policije, BIA i VBA za presretanjem ili pristupu zadržanim podacima. Operator nema zakonsku obavezu da odredi takva lica i da ona dobiju bezbjednosni sertifikat.[16] *Ona bi, međutim, morala bi imati posebnu obuku i dozvolu, s obzirom da dolaze u dodir sa tajnim podacima.*

Konkretan zahtjev operatoru može da podnese samo ovlašćeno lice nadležnog organa, i to ako predoči adekvatan pravni osnov, odnosno sudsku odluku.[17] *To znači da je prilikom prijema zahtjeva operator dužan da ocijeni da li su svi preduslovi za pristup prisutni. Ako je u pitanju neovlašćeno lice ili nenadležni organ, te ako nema sudskog odobrenja, pristup se ne smije omogućiti.*[18] *Stoga je veoma važno da lica koja primaju zahtjeve na strani operatora imaju odgovarajuću obuku.*

Drugi problem je u tome što zainteresovanoj javnosti nije jasno predočeno da li VBA, BIA ili policija mogu direktno presretati komunikacije i pristupiti zadržanim podacima, dakle bez prethodnog podnošenja zahtjeva, čak i bez znanja operatora. Ovo je važno jer su operatori dužni samo da bilježe primljene zahtjeve za presretanje, odnosno za pristup podacima, zbog čega takvi direktni pristupi ostaju van evidencije. Ipak, čini se da formulacija iz ZEK-a ostavlja mogućnost ostvarivanja direktnog pristupa. Nadležni organ, naime, obraća se operatoru zahtjevom kada ne može da primijeni mjeru bez pristupa prostorijama,

---

15 Riječ je o Pravilniku o zahtevima za uređaje i programsku podršku za zakonito presretanje komunikacija i zadržavanje podataka o elektronskim komunikacijama. Kao podzakonski akt morao je da čeka neophodne izmjene neustavnih odredbi ZEK-a do kojih je došlo u junu 2014.

16 Neusvojeni Pravilnik takvu obavezu predviđa u članu 20. Pogledati čl. 42 Zakona o tajnosti podataka, ("Sl. glasnik RS", br. 104/2009).

17 Zanimljivo je da, iako je sudsko odobrenje jedan od glavnih uslova za primjenu obje mjere, u nastavku Zakona o elektronskim komunikacijama sudska odluka kao pravni osnov pominje se samo za pristup zadržanim podacima, dok se za presretanje navodi samo "akt" uopšte. Nije jasno zašto oba puta nije upotrijebljena ista formulacija (V. čl.126-128 ZEK).

18 Član 130(2)(3) ZEK.

mreži, pripadajućim sredstvima ili opremi operatora (dakle ne uvijek, već samo u naročitim okolnostima).[19]

Poverenik za zaštitu podataka o ličnosti je u julu 2012. otkrio ne samo da se javljaju pristupi zadržanim podacima bez upućivanja zahtjeva operatoru, nego i da je njihov broj daleko veći od broja podnesenih zahtjeva. Međutim, samo je jedan od nadziranih operatora mobilne telefonije imao podatke o takvim pristupima.[20] *Neophodno je da svi operatori razviju softvere koji bi, na sličan način, čuvali neizbrisiv trag o svakom pristupu zadržanim podacima, odnosno presretanju komunikacija.*[21]

KOLIKO DUGO?

Primjena ovih mjera ima rok trajanja, i to najduže 12 mjeseci, što je ekvivalentno sa obavezom operatora da zadržane podatke čuvaju 12 mjeseci od dana obavljene komunikacije. Nijedan zakon, međutim, ne daje ovo maksimalno trajanje na prvi mah. Rok je uvijek kraći, sa mogućnostima produženja u posebnim okolnostima. Tako ZKP nudi formulu 3+3+2x3 (prvobitna tri mjeseca mogu se produžiti za još tri zbog neophodnosti daljeg prikupljanja podataka; a ako je riječ o krivičnim djela organizovanog kriminala ili ratnog zločina izuzetno se mogu produžiti još dva puta po tri mjeseca). Za VBA i policiju određen je rok 6+6 mjeseci, a za BIA 3+3x3 mjeseca (prvobitno trajanje od tri mjeseca može se još najviše tri puta produžiti za po tri mjeseca).[22] Inače, važi pravilo da se mjere primjenjuju dok za to postoje razlozi, što znači da se mogu obustaviti i prije isteka roka, ali i da se ne smiju produžavati izvan roka, čak i kad ti razlozi nisu prestali.

KO NADZIRE?

Rad policije, VBA i BIA pod lupom je unutrašnjih i spoljnih nadzirača. Unutrašnji nadzirači su: Sektor unutrašnje kontrole policije, Unutrašnja kontrola VBA i Unutrašnja i budžetska kontrola BIA.[23] Izričito ovlašćenje da nadzire zakonitost primjene posebnih mjera od strane VBA ima i Generalni inspektor.[24]

---

19 Članovi 127(3) i 128(8) ZEK-a.

20 Godišnji izveštaj Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti za 2012. godinu, Beograd, mart 2013., str. 60. Dostupno na: http://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/izvestaj2012final.pdf (pristup 4. novembra 2014.)

21 Ova obaveza predviđena je članom 17 neusvojenog Pravilnika.

22 V. Član 167 ZKP, član 17 ZVBA i VOA, član 83 ZP, član 15a ZBIA.

23 V. Član 171 Zakona o policiji, te član 57 Zakona o VBA i VOA. Unutrašnja kontrola BIA, međutim, nije zakonska kategorija (v. http://www.bia.gov.rs/rsl/o-agenciji/organizaciona-struktura.html).

24 Član 54(2) Zakona o VBA i VOA.

U spoljne nadzirače spadaju sudovi, Narodna skupština i nezavisna regulatorna tijela. Nadležni sudovi vrše kontrolu prvenstveno kroz neophodno prethodno ili naknadno odobravanje primjene mjera.[25] Samo ako se one primjenjuju zbog potreba vođenja krivičnog postupka, nadležni sudija (sudija za prethodni postupak) prima prikupljeni materijal sa izvještajem.[26] Narodna skupština vrši nadzor preko dva nadležna odbora. Međutim, za razliku od Odbora za kontrolu službi bezbednosti koji je eksplicitno ovlašćen da nadzire zakonitost primjene posebnih mjera od strane VBA i BIA, Odbor za odbranu i unutrašnje poslove ima samo uopštene nadležnosti za nadzor nad radom MUP-a.[27]

S obzirom da zadržani elektronski podaci spadaju u podatke o ličnosti, koji uživaju posebnu ustavnu i zakonsku zaštitu, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti nadzire rukovanje njima. Štaviše, takav nadzor sproveden je već dva puta, nad operatorima mobilne telefonije u 2012., a nad internet provajderima u 2014. godini.[28] Zaštitnik građana vrši nadzor nad primjenom posebnih mjera u okviru svoje nadležnosti staranja o zaštiti ljudskih prava.

Da bi nadzor bio moguć, svako presretanje komunikacija i pristup zadržanim podacima mora da se evidentira. Nadležni organi (policija, VBA, BIA) i operatori vode zasebne tajne evidencije o presretnutim komunikacijama i o pristupu/dostavljanju zadržanih podataka. Evidencije primjenjivača mjera sadrže određenje pravnog osnova, te datum i vrijeme korišćenja mjere, a evidencije operatora sadrže još i identifikaciju ovlašćenog lica koje podnosi zahtjev za presretanje, odnosno pristup podacima.[29]

Takođe, nadležni organi i operatori vode dodatno evidencije o zahtjevima za pristup zadržanim podacima na godišnjem nivou i dostavljaju je Povereniku za pristup informacijama od javnog značaja i zaštitu podataka o ličnosti. Ove evidencije su sasvim uopštene, ne sadrže nikakve detalje, i tiču se samo zahtjeva za pristup podacima, ne i presretanja komunikacija. Zato na njima, za razliku od prethodno navedenih, ne stoji oznaka tajnosti. One sadrže informacije o ukupnom broju podnijetih i ispunjenih zahtjeva, kao i o vremenu između dana zadržavanja podataka do dana kad su zatraženi.[30]

---

25 U slučaju hitnosti ili naknadnog proširenja mjere, sud odobrenje daje nakon početka primjene mjere, odnosno njenog proširenja.

26 Član 170 Zakonika o krivičnom postupku. Dostavljanje prikupljenih podataka nadležnom sudiji predviđa i Zakon o policiji (član 83). U matičnim zakonima o VBA i BIA ova obaveza se ne spominje.

27 Član 66 Poslovnika Narodne skupštine Republike Srbije, član 52 ZVBA i VOA, član 17 ZBIA. Pogledati i članove 9 i 170 ZP.

28 http://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/izvestaj2012final.pdf; http://www.poverenik.rs/sr/saopstenja-i-aktuelnosti/1764-zabrinjavajuci-rezultati-nadzora-nad-operatorima-interneta.html (pristup 4.11.2014.)

29 Članovi 127 i 128 ZEK.

30 Član 130a ZEK.

ŠTA POSLIJE?

Lica prema kojima su primjenjivane ove posebne mjere generalno ne mogu o tome naknadno saznati. Očigledan izuzetak su lica protiv kojih se u krivičnom postupku upotrijebe rezultati tajnog nadzora komunikacija kao dokazi. Takođe, nadležni sudija može (a ne mora) obavijestiti lice da je bilo objekt posebne mjere, ako javni tužilac u roku od šest mjeseci ne iskoristi materijal prikupljen tim putem, a procijeni da takvo obavještenje neće ugroziti mogućnost vođenja krivičnog postupka.[31]

Svi podaci o predlaganju, odlučivanju i primjeni specijalnih mjera presretanja komunikacija i pristupa zadržanim elektronskim podacima imaju oznaku tajnosti, što znači da im može pristupiti samo uzak krug subjekata koje na to ovlašćuje Zakon o tajnosti podataka.[32] Treba imati u vidu, međutim, da specijalnu mjeru čini pristup zadržanim elektronskim podacima, a ne sâmo zadržavanje podataka, koje predstavlja stalnu obavezu svakog operatora i preduslov za mogućnost pristupa. Svako ko koristi neku uslugu elektronske komunikacije, može da računa s tim da se podaci o njoj zadržavaju, ali ne može da sazna da li je neko tražio ili ostvario pristup njima.

Nezakonito prikupljeni i neupotrijebljeni podaci se uništavaju. Uništava se sav materijal prikupljen primjenom ovih mjera na način koji nije zakonom propisan, odnosno nije u kratkom roku naknadno odobren od strane nadležnog suda, bilo da se radi o krivičnom postupku ili o zaštiti nacionalne bezbjednosti.[33] Takođe, uništava se i zakonito prikupljen materijal koji se ne iskoristi za svrhu radi koje je prikupljen.

Kada je riječ o procesuiranju krivičnih djela, uništava se materijal koji se za šest mjeseci ne iskoristi za pokretanje krivičnog postupka, ili za koji javni tužilac izjavi da neće iskoristiti. Ista je sudbina podataka do kojih je policija došla zakonitom primjenom specijalnih mjera radi hvatanja i privođenja lica a koja ne mogu biti dokazi u krivičnom postupku.[34]

Kako VBA i BIA čuvaju i uništavaju podatke zakonito prikupljene posebnim mjerama u cilju zaštite nacionalne bezbjednosti uređeno je podzakonskim aktima i internim pravilima.[35] Tako je Uputstvom o pravilima rada BIA, koje donosi direktor Agencije, predviđeno uništavanje podataka u nekoliko slučajeva: 1) ako nije potvrđena djelatnost prema kojoj je Agencija nadležna da postupa; 2) radi rasterećivanja dokumentacionih fondova, sukcesivno se uništavaju nepotrebni podaci; 3) prilikom brisanja pojedinih lica

---

31 Član 163 ZKP.

32 Pogledati u čl. 37-42 Zakona o tajnosti podataka ("Sl. glasnik RS", br. 104/2009).

33 Član 84, 163i 169 ZKP, član 15b ZBIA, član 15 ZVBAiVOA.

34 Član 163 ZKP, član 83 ZP.

35 V. Član 32 Zakona o VBA i VOA.

iz evidencija, na način predviđen internim Pravilnikom o izveštavanju, dokumentaciji i evidencijama u BIA.[36]

Takođe, operator je dužan da uništi sve elektronske podatke koje je zadržao, a kojima nije pristupano u roku od 12 mjeseci.[37]

POGLED IZ EU?

Članice Evropske unije bile su obavezane direktivom iz 2006. godine (2006/24/EC) da nametnu provajderima elektronskih komunikacija zakonsku obavezu zadržavanja podataka o komunikaciji u trajanju najmanje šest mjeseci, a najviše dvije godine. Nakon ozbiljnih kampanja nevladinog sektora i negativnih sudskih presuda na nacionalnom nivou (npr. Njemačka, Češka, Rumunija), direktiva je najzad u aprilu 2014. godine proglašena nevažećom od strane Evropskog suda pravde (C-293/12 and C-594/12). Sud je utvrdio da direktiva propisuje zadiranje u pravo na privatnost i na zaštitu ličnih podataka, zajemčene Poveljom osnovnih prava EU, nesrazmjerno razlozima koje navodi (sprečavanje, otkrivanje, istraga i procesuiranje težih krivičnih djela). Direktiva, naime, ne reguliše precizno razloge za pristup zadržanim podacima, niti predviđa prethodnu sudsku kontrolu. Period čuvanja 6-24 mjeseci je preopširno zadat, a nigdje se ne zahtjeva da se podaci čuvaju samo unutar EU. Sud je stoga zaključio da su rizici ka zloupotrebama visoki.

To što direktiva EU odnedavno ne važi, ne znači da se automatski ukidaju nacionalni zakoni doneseni na osnovu nje. Posljedica presude ESP-a je samo da države članice više nemaju obavezu da ovu direktivu sprovode. One sopstvene zakone mogu ukinuti, izmijeniti ili staviti pred domaću provjeru ustavnosti.

---

36 Bezbednosno-informativna agencija. Odgovor na upitnik BCBP-a. Beograd, 30. 5. 2012.

37 Član 130(4) ZEK.

UKRATKO

ŠTA?
Zakonito presretanje komunikacija (uvid u sadržaj komunikacije) i pristup zadržanim elektronskim podacima (bitni podaci o komunikaciji, bez uvida u sadržaj)

KO?
Vojnobezbednosna agencija (VBA), Bezbednosno-informativna agencija (BIA) i policija

ZAŠTO?
Za potrebe vođenja krivičnog postupka i zaštitu bezbjednosti Republike Srbije

KAKO?
Na osnovu odluke nadležnog suda i samo na određeno vrijeme

KOLIKO DUGO?
Dok postoje razlozi za primjenu, najduže 12 mjeseci

KO NADZIRE?
Organi unutrašnje kontrole, te nadležni sudovi, Narodna skupština preko Odbora za odbranu i unutrašnje poslove i Odbora za kontrolu službi bezbednosti, i nezavisna regulatorna tijela – Poverenik i Zaštitnik građana..

ŠTA POSLIJE?
Lica prema kojima su mjere primijenjene generalno ne mogu o tome saznati naknadno. Nezakonito prikupljeni i neupotrijebljeni podaci se uništavaju

RELEVANTNI PRAVNI OKVIR

Ustav Republike Srbije („Sl. glasnik RS", br. 98/2006)

Zakon o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014) – ZEK

Zakonik o krivičnom postupku ("Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014) – ZKP

Zakon o Bezbednosno-informativnoj agenciji („Službeni glasnik RS", br. 42/2002, 111/2009, 65/2014 - US, 66/2014.) – Zakon o BIA

Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji (("Sl. glasnik RS", br. 88/2009, 55/2012 – odluka US i 17/2013)– Zakon o VBA i VOA

Zakon o policiji ("Sl. glasnik RS", br. 101/2005, 63/2009 - odluka US i 92/2011)- ZP

O AUTORKI

Jelena Pejić je stažistkinja XVI generacije stažista i stažistkinja u BCBP. Diplomirala je međunarodne odnose na Fakultetu političkih nauka u Beogradu 2014. Trenutno je studentkinja master studija Humanitarno pravo i pravo ljudskih prava na istom fakultetu.

www.bezbednost.org