

**Opravična št.:**

U-I-65/13

ECLI:

ECLI:SI:USRS:2014:U.I.65.13

Akt:

Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12 in 110/13) (ZEKom-1), 162, 163, 163.1, 164, 165, 166, 167, 168 in 169 čl.

Izrek:

Členi 162, 163, 164, 165, 166, 167, 168 in 169 Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12 in 110/13) se razveljavijo. Operaterji iz prvega odstavka 163. člena Zakona o elektronskih komunikacijah morajo nemudoma po objavi te odločbe v Uradnem listu Republike Slovenije uničiti vse podatke, ki jih hranijo na podlagi izpodbijanih določb.

Evidenčni stavek:

Z določitvijo obvezne in neselektivne hrambe nekaterih prometnih podatkov vseh komunikacij pri telefoniji v fiksnem omrežju, mobilni telefoniji, pri dostopu do interneta, internetne elektronske pošte in internetne telefonije (za 14 oziroma 8 mesecev) nastajajo pri operaterjih obsežne zbirke osebnih podatkov uporabnikov teh storitev, iz katerih je mogoče izluščiti zelo natančne ugotovitve o njihovem zasebnem življenju. Takšna obdelava osebnih podatkov pomeni poseg v pravico posameznika do varstva osebnih podatkov (prvi odstavek 38. člena Ustave).

Obvezna in neselektivna hramba prometnih podatkov pomeni izrazit poseg v pravico do varstva osebnih podatkov zaradi obsega oseb, ki jih ukrep prizadene, in narave podatkov, ki se hranijo, ter dejstva, da se z nastankom obsežnih zbirk osebnih podatkov celotne populacije izrazito poveča tveganje nezakonitega dostopa do teh podatkov. Invazivnost posega izostri tudi dejstvo, da osebe, katerih podatki se hranijo, o hrambi in morebitni kasnejši uporabi podatkov niso obveščene, zato lahko hramba podatkov pri njih ustvari neoprijemljivi občutek stalnega nadzora, to pa lahko vpliva na izvrševanje drugih pravic, predvsem pravice do svobodnega izražanja in obveščanja (prvi odstavek 39. člena Ustave).

Za poseg v pravico do varstva osebnih podatkov je imel zakonodajalec ustavno dopusten cilj, in sicer preprečevanje, preiskovanje in pregon hudih oblik kaznivih dejanj, obramba države in zaščita državne varnosti z namenom zagotavljanja varstva človekovih pravic in temeljnih svoboščin ter drugih temeljnih pravnih dobrin pred protipravnimi napadi nanje.

Izpodbijani ukrep je tudi primeren za doseg navedenih ciljev, čeprav v določenih primerih zaradi tehničnih obvodov ali posebnih načinov uporabe telekomunikacijskih storitev, ki omogočijo anonimno uporabo, cilja v določenem obsegu ni mogoče doseči. Ukrep je neprimeren, kadar sredstvo za doseg cilja ni v razumni zvezi s tem ciljem in kadar s sredstvom navedenega cilja v nobenem primeru ni mogoče doseči.

Izpodbijani ukrep ni nujno potreben. Obvezna in neselektivna hramba prometnih podatkov nujno pomeni, da se z njo posega v pretežni meri v pravice tistih, ki z nameni, zaradi katerih so bili v prvi vrsti ti podatki zbrani, nimajo oziroma ne bodo imeli niti posredne zveze in niso dali povoda za takšen

poseg v njihovo pravico do varstva osebnih podatkov. Hkrati se hranijo tudi podatki tistih komunikacij, katerih zaupna oziroma anonimna uporaba je nujna za doseg njihovega namena. Izpodbijana ureditev ni zamejila hrambe podatkov na določeno časovno obdobje, geografsko območje ali krog oseb, ki bi lahko bile v določeni zvezi z namenom, ki ga ukrep zasleduje. Zakonodajalec tudi ni pojasnil razlogov za določitev roka hrambe v dolžini 14 mesecev za podatke v zvezi z javno dostopnimi telefonskimi storitvami oziroma 8 mesecev za druge podatke in s tem tudi ne razlogov, zakaj krajši rok hrambe ne bi zadostil namenu, ki ga zasleduje. Ukrep tudi ni nujno potreben, ker zakonodajalec obdelave osebnih podatkov ni zamejil le na preiskovanje, odkrivanje in pregon hudih kaznivih dejanj. Ker je zakonodajalec z določitvijo obvezne hrambe prometnih podatkov izrazilo posegel v pravico do varstva osebnih podatkov, hkrati pa ni skrbno odmeril okoliščin, na podlagi katerih bi ta poseg zamejil le na tisto, kar je še nujno potrebno za doseg namena, je s tem nesorazmerno posegel v pravico do varstva osebnih podatkov iz prvega odstavka 38. člena Ustave. Zato je izpodbijana ureditev protiustavna.

Geslo:

1.5.51.1.17.1 - Ustavno sodstvo - Odločbe - Vrste odločitev Ustavnega sodišča - V postopku abstraktne presoje - Razveljavitev - Zakona.

1.5.51.1.22 - Ustavno sodstvo - Odločbe - Vrste odločitev Ustavnega sodišča - V postopku abstraktne presoje - Določitev načina izvršitve odločbe.

2.1.1.3 - Viri ustavnega prava - Razredi - Pisani viri - Pravo Skupnosti.

2.1.3.2.2 - Viri ustavnega prava - Razredi - Sodna praksa - Mednarodna sodna praksa - Sodišče Evropskih skupnosti.

2.1.1.4.3 - Viri ustavnega prava - Razredi - Pisani viri - Mednarodni dokumenti - Evropska konvencija o človekovih pravicah iz leta 1950.

2.1.1.4.14 - Viri ustavnega prava - Razredi - Pisani viri - Mednarodni dokumenti - Listina Evropske unije o temeljnih pravicah.

5.3.30.1 - Temeljne pravice - Državlanske in politične pravice - Pravica do zasebnega življenja (35, 36, 37) - Varstvo osebnih podatkov (38).

3.9 - Splošna načela - Vladavina prava.

3.16 - Splošna načela - Sorazmernost.

Pravna podlaga:

Člen 2, 5, 15.3, 38, 38.1, 39, 39.1, Ustava [URS]

Člen 8, Konvencija o varstvu človekovih pravic in temeljnih svoboščin [EKČP]

Člen 4, 5, Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov [MKVP]

Člen 40.2, 43, Zakon o Ustavnem sodišču [ZUstS]

Opomba:

⌘

Dokument v PDF obliki:



[U-I-65-13_vmesni sklep.pdf](#)

[U-I-65-13.pdf](#)

Polno besedilo:

U-I-65/13-16

26. 9. 2013

Ustavno sodišče je v postopku za oceno ustavnosti, začetem z zahtevo Informacijskega pooblaščenca, na seji 26. septembra 2013

sklenilo:

Postopek za oceno ustavnosti 162. do 169. člena Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12) se prekine do odločitve Sodišča Evropske unije v zadevah C-293/12 in C-594/12.

OBRAZLOŽITEV

A.

1. Predlagatelj zahteva presojo ustavnosti 162. do 169. člena Zakona o elektronskih komunikacijah (nadaljevanju ZEKom-1), ki je začel veljati 15. 1. 2013. Z izpodbijanimi določbami je Republika Slovenija prenesla v svoj pravni red Direktivo 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13. 4. 2006, str. 54 – v nadaljevanju Direktiva o hrambi podatkov). Izpodbijana ureditev nalaga obveznost ponudnikom javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, da hranijo določene prometne, lokacijske in druge podatke, potrebne za določitev posameznika (164. člen ZEKom-1), in sicer za namene, kot jih predvideva zakon, ki ureja kazenski postopek, zakon, ki ureja delovanje Slovenske obveščevalno-varnostne agencije, in zakon, ki ureja obrambo države (prvi odstavek 162. člena ZEKom-1). Podatki se hranijo 14 mesecev od dneva komunikacije (podatki v zvezi z javno dostopnimi telefonskimi storitvami) oziroma 8 mesecev od dneva komunikacije (drugi podatki). Izjemoma se lahko določi daljša doba (peti in šesti odstavek 163. člena ZEKom-1). Določeni so raven zavarovanja hrambe podatkov in ukrepi, ki jih mora operater sam ali v sodelovanju z drugimi sprejeti v zvezi s hrambo podatkov (165. člen ZEKom-1). Določena je tudi nadzorna vloga Informacijskega pooblaščenca (169. člen ZEKom-1).

2. Temeljni očitke zahteve za oceno ustavnosti je, da je Republika Slovenija na podlagi Direktive o hrambi podatkov naložila operaterjem obvezno hrambo prometnih in lokacijskih podatkov vseh uporabnikov na zalogo, torej ne glede na to, ali so uporabniki sami dali povod za tak poseg v njihove pravice. Sklicujoč se na ustavnosodno presojo in prakso Evropskega sodišča za človekove pravice, predlagatelj opozarja, da ne le vsebina komunikacije, temveč tudi podatki, ki so integralni del komunikacije, uživajo ustavnopravno in konvencijsko varstvo. Hramba podatkov na zalogo naj bi pomenila nedopustne posege v pravico do varstva osebnih podatkov (38. člen Ustave) in komunikacijske zasebnosti (37. člen Ustave), posledično pa tudi v pravico do svobode gibanja (32. člen Ustave), pravico do svobode izražanja (39. člen Ustave) in v načelo domnevne nedolžnosti (27. člen Ustave). Meni, da ti posegi ne prestanejo testa sorazmernosti v skladu z ustaljeno ustavnosodno presojo.

3. Zahteva za oceno ustavnosti je bila poslana Državnemu zboru in Vladi. Državni zbor se v odgovoru strinja, da hramba podatkov iz 164. člena ZEKom-1 občutno posega v zasebnost posameznika, vendar opozarja, da je hramba podatkov pomembno orodje za odkrivanje in preiskovanje kaznivih dejanj in da je največkrat treba podatke pridobiti za nazaj, kar omogoča prav obvezna hramba podatkov na zalogo. Državni zbor opozarja še na določbe izpodbijane ureditve, ki zmanjšujejo možnost zlorab.

Vlada v mnenju med drugim navaja, da predlagatelj, čeprav izrecno izpodbija določbe nacionalnega predpisa, po vsebini zatrjuje neskladje Direktive o hrambi podatkov z navedenimi človekovimi pravicami.

4. Odgovor Državnega zbora in Vlade sta bila predložena predlagatelju. V odgovoru predlagatelj vztraja, da ukrep ni sorazmeren. Meni, da opravljene raziskave ne potrjujejo, da hramba podatkov pripomore k večji preiskanosti kaznivih dejanj. Opozarja tudi, da je z enostavnimi tehničnimi obvodi mogoče doseči, da ukrep ne bo učinkovit. Zato naj tako občuten poseg v zasebnost uporabnikov komunikacijskih storitev ne bi bil sorazmeren ciljem, ki jim sledi.

B.

5. Predlagatelj izrecno izpodbija samo obveznost hrambe podatkov, ki izhaja iz Direktive o hrambi podatkov in glede katere Direktiva državam članicam ne daje možnosti drugačne ureditve. Zato predlagatelj dejansko zatrjuje neskladje Direktive o hrambi podatkov s človekovimi pravicami, na kar izrecno opozarja tudi Vlada. Pri tem Ustavno sodišče šteje, da se v temelju zatrjevana protiustavnost nanaša predvsem na pravici do komunikacijske (37. člen Ustave) in informacijske zasebnosti (38. člen Ustave). Argumentacija, da zaradi tako hudega posega v navedeni pravici prihaja posledično tudi do ogrožanja pravice do svobode izražanja (39. člen Ustave), pravice do svobode gibanja (32. člen Ustave) in domneve nedolžnosti (27. člen Ustave), pa v svojem bistvu pomeni poudarjanje nesorazmerne teže posega v pravico do zasebnosti. Človekove pravice, ki jih urejata 37. in 38. člen Ustave, so v pravu Evropske unije zagotovljene kot temeljne pravice v 7. in 8. členu Listine Evropske unije o temeljnih pravicah (UL C 326, 26. 10. 2012 – v nadaljevanju Listina). Zato gre dejansko za vprašanje skladnosti določb Direktive o hrambi podatkov z navedenimi določbami Listine.

6. Republika Slovenija je s pristopom k Uniji na podlagi 3.a člena Ustave prenesla izvrševanje dela suverenih pravic na Evropsko unijo.[1] Iz tretjega odstavka 3.a člena Ustave izhaja, da se pravni akti in odločitve, sprejeti v okviru Evropske unije, uporabljajo v skladu s pravno ureditvijo Evropske unije.[2] Ta določba zavezuje tudi Ustavno sodišče, da pri izvrševanju svojih pristojnosti upošteva pravo Evropske unije tako, kot to iz njega izhaja. Izpodbijane določbe ZEKom-1 prenašajo obveznosti, ki jih nalaga Direktiva o hrambi podatkov, torej njihovo izvrševanje pomeni uporabo prava Evropske unije. V skladu s prvim odstavkom 51. člena Listine so države članice zavezane z njenimi določbami, kadar uporabljajo pravo Evropske unije.

7. Ustavno sodišče je že sprejelo stališče, da njegova pristojnost za presojo ustavnosti predpisov, ki implementirajo direktive v notranji pravni red, ni izključena.[3]

8. Glede na to, da očitki o protiustavnosti zakonskih določb po vsebini pomenijo očitek o neskladnosti določb Direktive o hrambi podatkov s 7. in 8. členom Listine, je odločitev o veljavnosti Direktive o hrambi podatkov ključnega pomena za presojo ustavnosti določb nacionalne zakonodaje. O veljavnosti Direktive je na podlagi točke b) prvega odstavka 267. člena Pogodbe o delovanju Evropske unije (UL C 326, 26. 10. 2012 – v nadaljevanju PDEU) izključno pristojno presojati Sodišče Evropske unije.[4]

9. O veljavnosti Direktive o hrambi podatkov zaradi njene skladnosti s 7. in 8. členom Listine Sodišče Evropske unije še ni odločilo. Vprašanje o veljavnosti Direktive o hrambi podatkov je sicer že bilo predloženo Sodišču Evropske unije v predhodno odločanje v zadevi C-301/06,[5] vendar se je ta zadeva nanašala le na vprašanje pravne podlage te Direktive. Vprašanje o veljavnosti Direktive z vidika 7. in 8. člena Listine je postavljeno tudi v zadevah C-293/12[6] in C-594/12.[7] Navedena postopka pred Sodiščem Evropske unije že potekata, opravljena je bila že ustna obravnava, določen je

tudi datum generalnemu pravobranilcu za predložitev sklepnih predlogov v zadevah. Ker se zatrjevana protiustavnost po vsebini ujema z razlogi, zaradi katerih že poteka postopek odločanja o veljavnosti Direktive o hrambi podatkov, Ustavnemu sodišču ni treba vložiti predloga za predhodno odločanje Sodišču Evropske unije.

10. Ustavno sodišče o zadevi ne more odločiti, dokler Sodišče Evropske unije, ki je izključno pristojno presoјati veljavnost navedene direktive, ne odloči o njeni veljavnosti. Zato je Ustavno sodišče do odločitve Sodišča Evropske unije v navedenih zadevah prekinilo postopek odločanja o ustavnosti izpodbijanih določb ZEKom-1.

C.

11. Ustavno sodišče je sprejelo ta sklep na podlagi točke b) prvega odstavka 267. člena PDEU v zvezi s tretjim odstavkom 3.a člena Ustave in drugega odstavka 41. člena Zakona o Ustavnem sodišču (Uradni list RS, št. 64/07 – uradno prečiščeno besedilo in 109/12 – ZUstS) v sestavi: predsednik dr. Ernest Petrič ter sodnice in sodniki dr. Mitja Deisinger, dr. Dunja Jadek Pensa, mag. Marta Klampfer, dr. Etelka Korpič – Horvat, mag. Miroslav Mozetič, Jasna Pogačar in dr. Jadranka Sovdat. Sklep je sprejelo soglasno.

dr. Ernest Petrič
Predsednik

Opombe:

[1] Pogodba med Kraljevino Belgijo, Kraljevino Dansko, Zvezno republiko Nemčijo, Helensko republiko, Kraljevino Španijo, Francosko republiko, Irsko, Italijansko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko, Republiko Avstrijo, Portugalsko republiko, Republiko Finsko, Kraljevino Švedsko, Združenim kraljestvom Velike Britanije in Severne Irske (državami članicami Evropske unije) in Češko republiko, Republiko Estonijo, Republiko Ciper, Republiko Latvijo, Republiko Litvo, Republiko Madžarsko, Republiko Malto, Republiko Poljsko, Republiko Slovenijo in Slovaško republiko o pristopu Češke republike, Republike Estonije, Republike Ciper, Republike Latvije, Republike Litve, Republike Madžarske, Republike Malte, Republike Poljske, Republike Slovenije in Slovaške republike k Evropski uniji (UL L 236, 23. 9. 2003, in Uradni list RS, št. 12/04, MP, št. 3/04 – MPPEU).

[2] Tretji odstavek 3.a člena Ustave določa: "Pravni akti in odločitve, sprejeti v okviru mednarodnih organizacij, na katere Slovenija prenese izvrševanje dela suverenih pravic, se v Sloveniji uporabljajo v skladu s pravno ureditvijo teh organizacij."

[3] Glej sklep Ustavnega sodišča št. U-I-113/04 z dne 7. 2. 2007 (Uradni list RS, št. 16/07, in OdlUS XVI, 16) in odločbo Ustavnega sodišča št. U-I-37/10 z dne 18. 4. 2013 (Uradni list RS, št. 39/13).

[4] Tako tudi že Ustavno sodišče v sklepu št. U-I-113/04 z dne 8. 7. 2004.

[5] Glej sodbo v zadevi *Irška proti Evropskemu parlamentu in Svetu EU*, C-301/06, z dne 10. 2. 2009.

[6] Predlog za sprejetje predhodne odločbe, ki ga je vložilo High Court of Ireland 11. junija 2012 – *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*.

[7] Predlog za sprejetje predhodne odločbe, ki ga je vložilo Verfassungsgerichtshof (Avstrija) 19. decembra 2012 – *Kärntner Landesregierung in drugi*.

U-I-65/13-19

3. 7. 2014

ODLOČBA

Ustavno sodišče je v postopku za oceno ustavnosti, začetem z zahtevo Informacijskega pooblaščenca, na seji 3. julija 2014

odločilo:

1. Členi 162, 163, 164, 165, 166, 167, 168 in 169 Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/12 in 110/13) se razveljavijo.

2. Operaterji iz prvega odstavka 163. člena Zakona o elektronskih komunikacijah morajo nemudoma po objavi te odločbe v Uradnem listu Republike Slovenije uničiti vse podatke, ki jih hranijo na podlagi izpodbijanih določb.

OBRAZLOŽITEV

A.

1. Informacijski pooblaščenec vlaga na podlagi šeste alineje 23.a člena Zakona o Ustavnem sodišču (Uradni list RS, št. 64/07 – uradno prečiščeno besedilo in 109/12 – v nadaljevanju ZUstS) zahtevo za oceno ustavnosti 162. do 169. člena Zakona o elektronskih komunikacijah (v nadaljevanju ZEKom-1), ki je začel veljati 15. 1. 2013. Z izpodbijanimi določbami je Republika Slovenija prenesla v svoj pravni red Direktivo 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13. 4. 2006 – v nadaljevanju Direktiva o hrambi podatkov).[1]

2. Predlagatelj je nadzorni organ za nadzor izvajanja določb o obvezni hrambi podatkov v skladu z določbami XIII. poglavja ZEKom-1 (169. člen ZEKom-1). Zatrjuje, da vodi inšpekcijski postopek nad ravnanjem enega od slovenskih mobilnih operaterjev po določbah ZEKom-1. Ker je v tem postopku podvomil o ustavnosti določb, na podlagi katerih je operater shranjeval prometne, lokacijske ter z njimi povezane podatke (v nadaljevanju prometni podatki) uporabnikov na podlagi prvega odstavka 163. člena ZEKom-1, je vložil zahtevo za oceno ustavnosti izpodbijanih določb.

3. Temeljni očitki zahteve za oceno ustavnosti izpodbijanih določb je, da je Republika Slovenija na podlagi Direktive o hrambi podatkov naložila operaterjem obvezno hrambo podatkov vseh uporabnikov na zalogo, torej ne glede na to, ali so uporabniki sami dali povod za tak poseg v njihove pravice. Taka hramba podatkov naj bi pomenila nedopustne posege v pravico do varstva osebnih podatkov (38. člen Ustave), v komunikacijsko zasebnost (37. člen Ustave), posledično pa tudi v

pravico do svobode gibanja (32. člen Ustave), pravico do svobode izražanja (39. člen Ustave) in v načelo domnevne nedolžnosti (27. člen Ustave). Predlagatelj meni, da ti posegi ne prestopajo meja sorazmernosti v skladu z ustaljeno ustavnosodno presojo. Poudarja, da prometni podatki uživajo enako varstvo kot vsebina komunikacije in so varovani po 37. členu Ustave. Meni tudi, da posegi v pravice niso sorazmerni, ker empirični podatki ne dokazujejo, da bi bil namen takšne hrambe podatkov lahko dosežen s takim posegom v navedene pravice. Le pomembna višja stopnja raziskanosti hudih kaznivih dejanj naj bi upravičila prevlado javnega interesa nad interesi slehernega posameznika, da uživa zasebnost, se svobodno (nenadzorovano) giblje, komunicira, izraža mnenje ipd. Predlagatelj meni, da ukrep niti ni primeren, ker obstaja vrsta tehničnih obvodov, ki preprečujejo hrambo podatkov. Zavedanje uporabnikov, da je njihova komunikacija nadzorovana, po mnenju predlagatelja vpliva tudi na izvrševanje drugih pravic (predvsem na svobodo izražanja). Posameznik, ki ve, da je nadzorovan, se bo zaradi samocenzure obnašal drugače kot sicer. Predlagatelj meni, da je zaradi hrambe lokacijskih podatkov ureditev še dodatno invazivna, ker posega v svobodo gibanja. Zatrjuje tudi kršitev 3.a člena Ustave, ki jo vidi v tem, da je bila Direktiva o hrambi podatkov nepravilno prenesena v slovenski pravni red, ker dopušča hrambo prometnih podatkov tudi za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj, ki jih ni mogoče opredeliti kot hujša kazniva dejanja, in ker dopušča uporabo podatkov za namen zagotavljanja potreb obveščevalne službe in obrambe.

4. Državni zbor se v odgovoru na zahtevo sicer strinja, da hramba podatkov iz 164. člena ZEKom-1 občutno posega v zasebnost posameznika, vendar pa ne soglaša s stališčem predlagatelja, da teh podatkov država ne potrebuje. Opozarja, da je hramba podatkov pomembno orodje za odkrivanje in preiskovanje kaznivih dejanj, za obrambo države, nacionalno varnost in ustavno ureditev ter da je največkrat treba podatke pridobiti za nazaj, kar omogoča prav obvezna hramba na zalogo. Državni zbor opozarja na določbe izpodbijane ureditve, ki zmanjšujejo možnost zlorab, in sicer: desetletna hramba podatkov o dostopu do prometnih podatkov, operaterji morajo podatke hraniti in jih varovati kot zaupne v skladu z zakonom o tajnih podatkih, določene so sankcije za kršitev varnostnih pravil in dostop do podatkov je mogoč le na podlagi sodne odredbe.

5. Vlada v mnenju opozarja, da predlagatelj, čeprav izrecno izpodbija določbe nacionalnega predpisa, po vsebini zatrjuje neskladje Direktive o hrambi podatkov z navedenimi človekovimi pravicami. Vlada se ne strinja s stališčem, da sama hramba prometnih podatkov ni pomembno orodje za pregon kaznivih dejanj. Sklicuje se na Ocenjevalno poročilo o Direktivi o hrambi podatkov z dne 18. 4. 2011,[2] iz katerega naj bi izhajalo, da imajo shranjeni prometni podatki, kot jih predvideva Direktiva o hrambi podatkov, pomembno vlogo pri preiskovanju kaznivih dejanj. Enak sklep naj bi izhajal tudi iz analize glede uporabe podatkov o prometu elektronskih komunikacij za obdobje 2010–2012, ki jo je pripravila Policija. Iz te analize naj bi izhajalo, da imajo prometni podatki pomembno mesto pri zbiranju dokazov v okviru preiskave kaznivih dejanj, saj kažejo na posamezna dejstva, okoliščine, relacije, dinamike in vzorce, ki pomembno pripomorejo pri zbiranju temeljnih dokazov za neposredno dokazovanje suma storitve kaznivega dejanja (ugotavljanje načrtovanja kaznivih dejanj, ugotavljanje oseb in povezav v kriminalni združbi ipd). Vlada opozarja, da odkrivanje določenih kaznivih dejanj brez analize predhodno shranjenih podatkov niti ne bi bilo mogoče (npr. spolne zlorabe otrok, storjene po internetu). Poudarja tudi, da je dostop do prometnih podatkov pomembno orodje za boj proti terorizmu, mednarodno organizirani kriminaliteti in za delovanje obveščevalno-varnostne agencije z namenom varovanja varnosti države in njene ustavne ureditve. Vlada pojasnjuje, da operaterji hranijo prometne podatke v dveh ločenih zbirkah podatkov, v t. i. "komercialni" in v "retencijski" zbirki podatkov. Slednja je po obsegu manjša, saj se vanjo prenesejo iz komercialne zbirke podatkov le tisti podatki, ki jih taksativno določa 164. člen ZEKom-1. Posledica izpodbijane ureditve naj bi bil le daljši čas hrambe podatkov. Vlada meni, da izpodbijana ureditev ne posega v pravico do svobode ravnanja in gibanja ter v svobodo izražanja, kot ju opredelujeta 32. in 39. člen Ustave. Posegala pa naj bi v

pravico do komunikacijske in informacijske zasebnosti iz 37. in 38. člena Ustave pa tudi v splošno pravico do zasebnosti iz 35. člena Ustave, vendar naj bi bili ti posegi sorazmerni. Enako naj bi veljalo tudi za zatrjevano kršitev domneve nedolžnosti.

6. V odgovoru predlagatelj poudarja, da so navedbe Vlade o domnevni koristnosti obvezne hrambe podatkov pavšalne. Očita, da Vlada ne pojasni bistva: ali je zaradi uveljavitve obvezne hrambe prometnih podatkov prišlo do bistvene spremembe pri odkrivanju kaznivih dejanj v primerjavi z obdobjem, ko ureditev še ni veljala. Meni, da je analiza, ki jo je predložila Vlada, metodološko neustrezna in da zasleduje napačne cilje. Sklicuje se na študijo Inštituta Max Planck za tuje in mednarodno kazensko pravo iz leta 2011, iz katere naj bi izhajalo spoznanje, da hramba prometnih podatkov ne pripomore k večji preiskanosti kaznivih dejanj. Opozarja tudi na statistične podatke, ki jih je predložila Vlada in iz katerih izhaja, da je le manjši delež podatkov, ki jih potrebuje Policija, starejših od 6 mesecev. Opozarja tudi na dejstvo, da imajo storilci najtežjih kaznivih dejanj (predvsem organiziranih) znanje in sredstva, da učinkovito prikrijejo elektronske sledi. Posledica tega je, da bo izjemno obsežna zbirka podatkov celotne populacije namenjena le iskanju peščice najbolj nevednih in lahkomišelnih storilcev kaznivih dejanj, zaradi česar naj bi bili posegi očitno nesorazmeren ukrep.

B. - I.

7. Izpodbijane določbe so urejene v XIII. poglavju ZEKom-1 "Hramba podatkov". Ureditev, kot jo določa to poglavje, je zakonodajalec predvidel le zaradi prenosa zahtev Direktive o hrambi podatkov v nacionalni pravni red.[3] Obveznosti iz Direktive o hrambi podatkov je sicer slovenski zakonodajalec prvič prenesel v svoj pravni red že z uveljavitvijo Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (Uradni list RS, št. 129/06 – v nadaljevanju ZEKom-A),[4] ki je začel veljati 27. 12. 2006. Ureditev obvezne hrambe podatkov kot posledica implementacije Direktive o hrambi podatkov je (razen skrajšanja roka za hrambo podatkov z dveh let na sedaj veljavnih 14 oziroma 8 mesecev)[5] v praktično nespremenjeni obliki v veljavi že več kot 7 let.

8. Izpodbijane določbe operaterjem nalagajo obveznost shranjevanja podatkov v zvezi z uporabo določenih telekomunikacijskih storitev (telefonske storitve v fiksnem in mobilnem omrežju, dostop do interneta, elektronske pošte in internetne telefonije). Hranijo se podatki, na podlagi katerih se lahko ugotovi, kdo je komuniciral s kom, kdaj, koliko časa, kje in kako (164. člen ZEKom-1 in 5. člen Direktive o hrambi podatkov). Obveznost hrambe vključuje tudi neuspešne klice. Ne shranjuje se vsebina komunikacije (tretji odstavek 163. člena ZEKom-1 in prvi odstavek 3. člena Direktive o hrambi podatkov). Podatki se hranijo 14 mesecev od dneva komunikacije za podatke v zvezi z javno dostopnimi telefonskimi storitvami in 8 mesecev v zvezi z drugimi podatki. Izjemoma se lahko določi daljša doba hrambe (peti in šesti odstavek 163. člena ZEKom-1 ter 6. in 12. člen Direktive o hrambi podatkov). Po koncu hrambe mora operater podatke uničiti, razen tistih, za katere je bila izdana odredba za dostop in so bili posredovani pristojnemu organu (sedmi odstavek 163. člena ZEKom-1 in 7. člen Direktive o hrambi podatkov). Določeni so (na splošno) raven zavarovanja hrambe podatkov in ukrepi, ki jih mora operater sam ali v sodelovanju z drugimi sprejeti v zvezi s tem. Določena je tudi vloga Informacijskega pooblaščenca, ki lahko daje predhodna mnenja glede splošnega akta, ki podrobno določi način zavarovanja hrambe podatkov (165. člen ZEKom-1), in z določenimi omejitvami nadzira izvajanje določb poglavja XIII. ZEKom-1 (169. člen ZEKom-1). Operater mora podatke (če jih ustvari ali obdela pri zagotavljanju z njimi povezanih javnih komunikacijskih storitev) hraniti za namene pridobivanja podatkov v javnem komunikacijskem omrežju, ki jih določa zakon, ki ureja kazenski postopek, za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kakor jih določa zakon, ki ureja Slovensko obveščevalno-varnostno agencijo, in za obrambo države, kakor jo določa zakon, ki ureja obrambo države (prvi

odstavek 163. člena ZEKom-1 in v določenem obsegu tudi 1. člen Direktive o hrambi podatkov). Zagotovljena mora biti desetletna registracija dostopa do podatkov in posredovanja podatkov (peti odstavek 166. člena ZEKom-1). Dejstva, da bo oziroma da je do dostopa do podatkov in posredovanja podatkov prišlo, operater ne sme razkriti prizadeti osebi (ali tretjim), prav tako ne sme razkriti same sodne odredbe (četrti odstavek 166. člena ZEKom-1). To poglavje vsebuje tudi posebne določbe glede pomena izrazov, ki jih to poglavje uporablja (162. člen ZEKom-1), glede stroškov hrambe podatkov (167. člen ZEKom-1) in glede podatkov o odredbah o dostopu do podatkov in posredovanja podatkov (168. člena ZEKom-1).

9. Predlagatelj sicer izrecno izpodbija vse določbe XIII. poglavja ZEKom-1, vendar po vsebini, kot je razvidno iz 3. točke te obrazložitve, izpodbija le tiste določbe, ki nalagajo operaterjem obvezno hrambo določenih podatkov v javnem komunikacijskem omrežju (tudi) za namene in v obsegu, kot je to predvidela Direktiva o hrambi podatkov. V tem obsegu je Ustavno sodišče tudi opravilo presojo.

10. Predlagatelj je po vsebini dejansko zatrjeval neskladje Direktive o hrambi podatkov s človekovimi pravicami. Ustavno sodišče ni moglo odločiti o ustavnosti izpodbijane ureditve, dokler Sodišče Evropske unije, ki je izključno pristojno presojati veljavnost navedene direktive, ni odločilo o njeni veljavnosti. Postopek o zahtevi za oceno ustavnosti izpodbijanih določb ZEKom-1 je zato s sklepom št. U-I-65/13 z dne 26. 9. 2013 prekinilo do odločitve Sodišča Evropske unije v združenih zadevah št. C-293/12 in C-594/12, ki sta bili v času odločitve Ustavnega sodišča o prekinitvi postopka že v sklepni fazi odločanja.

11. Sodišče Evropske unije je s sodbo v združenih zadevah *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources in drugim ter Kärntner Landesregierung in drugi*, C-293/12 in C-594/12, z dne 8. 4. 2014 (v nadaljevanju sodba v združenih zadevah C-293/12 in C-594/12) Direktivo o hrambi podatkov razglasilo za neveljavno *ab initio*. Ocenilo je, da je zakonodajalec Evropske unije z njenim sprejetjem prekoračil meje, ki jih zahteva spoštovanje načela sorazmernosti, upošteva 7. in 8. člen ter prvi odstavek 52. člena Listine Evropske unije o temeljnih pravicah (UL C 326, 26. 10. 2012, str. 391 – v nadaljevanju Listina).

B. - II.

12. Z razglasitvijo Direktive o hrambi podatkov za neveljavno je odpadla obveznost države članice, da zahteve iz te direktive prenese v nacionalni pravni red. Vendar ostaja kljub temu varstvo prometnih podatkov tudi predmet ureditve v pravu Evropske unije. Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31. 7. 2002) v 5. in 6. členu nalaga državam članicam, naj zagotovijo zaupnost sporočil in s tem povezanih prometnih podatkov, če niso potrebni za namen prenosa sporočila ali če posameznik ni dal soglasja za takšno obdelavo. Ta direktiva v 15. členu omogoča, da: "[d]ržave članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, [...] te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive 95/46/ES. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje Skupnosti, vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji."

13. Hrambe prometnih podatkov za namene, kot jih določa prvi odstavek 163. člena ZEKom-1, torej pravo Evropske unije ne prepoveduje. Zato se država članica za ta ukrep lahko odloči. Če se odloči, pa mora spoštovati zahtevo po sorazmernosti ukrepa, v skladu z omejitvami iz navedene določbe Direktive. Slovenski zakonodajalec je torej s tega vidika upravičen določiti obvezno hrambo prometnih podatkov tudi za namene zaščite državne varnosti, obrambe, javne varnosti ter za preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj. V skladu z navedeno določbo Direktive pa mora tak poseg v temeljne pravice pomeniti potreben, primeren in ustrezen ukrep znotraj demokratične družbe. Tudi po ustaljeni ustavnosodni presoji mora za dopustnost posega v vsako človekovo pravico, in s tem tudi v pravico do informacijske zasebnosti iz prvega odstavka 38. člena Ustave, obstajati ustavno dopusten cilj, poseg pa mora biti tudi skladen z načeli pravne države, in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege države (splošno načelo sorazmernosti - 2. člen Ustave).[6] Dopustnost omejitve pravice do varstva osebnih podatkov je torej tudi po Ustavi urejena vsebinsko enako, kot izhaja iz 15. člena navedene direktive.

B. - III.

14. Na podlagi izpodbijane ureditve operaterji na zalogo (preventivno) in neselektivno shranjujejo taksativno določene prometne podatke vseh komunikacij pri telefoniji v fiksnem omrežju, mobilni telefoniji, pri dostopu do interneta, internetne elektronske pošte in internetne telefonije za določeno obdobje. Vlada navaja, da ti podatki kažejo na posamezna dejstva, okoliščine, relacije, dinamike in vzorce življenja posameznika. Glede na opredelitev v 1. točki 6. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 - uradno prečiščeno besedilo - v nadaljevanju ZVOP-1), ki določa sistem varstva osebnih podatkov, je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek, s tem da je fizična oseba določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa (2. točka 6. člena ZVOP-1). Na podlagi izpodbijane ureditve operaterji torej hranijo informacije, ki vsebujejo z vidika zasebnosti sporočila o določljivem posamezniku in morajo zato uživati varstvo osebnih podatkov, kot ga zagotavlja 38. člen Ustave. Ustavno sodišče se ne spušča v vprašanje, ali so prav vsi prometni podatki, ki jih določa izpodbijana ureditev, v vsakem primeru osebni podatki v smislu prej navedene opredelitve.[7] Ključno pa je, da je iz njih (skupaj) mogoče izluščiti podrobnosti iz življenja posameznika, in zato morajo uživati zaščito z vidika pravice do zasebnosti. Ali z besedami Sodišča Evropske unije v sodbi v združenih zadevah C-293/12 in C-594/12 (27. točka): "Na podlagi vseh teh podatkov je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi in socialna okolja, ki jih obiskujejo."

15. Hramba takih podatkov (tudi za namene, kot jih predvideva izpodbijana ureditev) pomeni glede na ustaljeno ustavnosodno presojo in tudi prakso Sodišča Evropske unije[8] poseg v pravico do varstva osebnih podatkov, ki jo zagotavljajo 38. člen Ustave, 8. člen Listine[9] in tudi 8. člen Konvencije o varstvu človekovih pravic in temeljnih svoboščin (Uradni list RS, št. 33/94, MP, št. 7/94 - v nadaljevanju EKČP).[10]

16. Iz ustaljene ustavnosodne presoje izhaja, da se v prvem odstavku 38. člena Ustave kot poseben vidik zasebnosti zagotavlja varstvo osebnih podatkov. Namen varstva osebnih podatkov je zagotoviti spoštovanje posebnega vidika človekove zasebnosti - t. i. informacijsko zasebnost. S tem ko Ustava to pravico posebej ureja, ji daje posebno mesto in pomen v siceršnjem varstvu zasebnosti posameznika.

Posebno mesto ima tudi na ravni Evropske unije. Listina je pravico do varstva osebnih podatkov v 8. členu tudi deklaratorno povzdignila med temeljne človekove pravice. Po ustaljeni ustavnosodni presoji pomeni vsako zbiranje in obdelovanje osebnih podatkov poseg v pravico do varstva zasebnosti oziroma v pravico posameznika, da obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni drugi. Temeljna vrednostna podstat te pravice je spoznanje, da ima posameznik pravico zadržati informacije o sebi zase in da je v izhodišču on tisti, ki odloča, koliko informacij o sebi bo razkril in komu.[11] Vendar pravica do informacijske zasebnosti ni neomejena, ni absolutna. Zato mora posameznik sprejeti omejitve informacijske zasebnosti oziroma dopustiti posege vanjo v prevladujočem splošnem interesu in ob izpolnjevanju ustavno določenih pogojev. Poseg je dopusten pod pogoji iz tretjega odstavka 15. člena in 2. člena Ustave. V tem okviru mora Ustavno sodišče presoditi, ali je zakonodajalec sledil ustavno dopustnemu cilju, če je ta podan, pa še, ali je omejitev skladna z načeli pravne države, in sicer s tistim izmed teh načel, ki prepoveduje prekomerne posege države (splošno načelo sorazmernosti).[12] V zakonu mora biti določno opredeljeno, kateri podatki se smejo zbirati in obdelovati, za kakšen namen jih je dovoljeno uporabiti, predvidena morata biti nadzor nad zbiranjem, obdelovanjem in uporabo osebnih podatkov ter varstvo tajnosti zbranih osebnih podatkov. Namen zbiranja osebnih podatkov mora biti ustavno dopusten. Zbirati se smejo le podatki, ki so primerni in nujno potrebni za uresničitev zakonsko opredeljenega namena.[13] Ko gre za obdelavo osebnih podatkov za namene policijskega dela, mora zakonodajalec še posebej skrbno pretehtati teža ukrepa, s katerim brez privolitve posameznika posega v občutljivo območje njegove zasebnosti.[14] To velja tudi za obdelavo osebnih podatkov v drugih državnih organih za potrebe obrambe države, nacionalne varnosti in ustavne ureditve.

17. Ustavno sodišče je že večkrat pojasnilo, da vsebinsko podobne zahteve kot 38. člen Ustave vsebuje tudi Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS, št. 11/94, MP, št. 3/94 – v nadaljevanju MKVP). Poleg tega, da morajo biti osebni podatki pridobljeni in obdelani pošteno in zakonito, MKVP terja sprejetje ukrepov, ki bodo zagotovili, da bodo osebni podatki shranjeni za določene in zakonite namene in da ne bodo uporabljeni na način, ki ni združljiv s temi nameni, ter da se bodo obdelovali le podatki, ki so primerni, ustrezni in niso pretirani glede na namen zbiranja (5. člen v zvezi s 4. členom MKVP).[15]

18. Prvi pogoj za dopustnost posega v pravico iz prvega odstavka 38. člena Ustave je torej obstoj ustavno dopustnega cilja. Temeljni namen Direktive o hrambi podatkov, zaradi katere je zakonodajalec izpodbijano ureditev vzpostavil, je bil določen v prvem odstavku 1. člena,[16] in sicer: "[...] da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic." Podobno tudi prvi odstavek 163. člena ZEKom-1 določa, da "mora [operater] za namene pridobivanja podatkov v javnem komunikacijskem omrežju, ki jih določa zakon, ki ureja kazenski postopek, za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kakor jih določa zakon, ki ureja Slovensko obveščevalno-varnostno agencijo, in za obrambo države, kakor jih določa zakon, ki ureja obrambo države, hraniti podatke iz 164. člena tega zakona, če jih ustvari ali obdela pri zagotavljanju z njimi povezanih javnih komunikacijskih storitev". Pregon hudih oblik kaznivih dejanj, obramba države in zaščita državne varnosti z namenom zagotavljanja varstva človekovih pravic in temeljnih svoboščin ter drugih temeljnih pravnih dobrin pred protipravnimi napadi nanje so ustavno dopustni cilji. Da lahko država na svojem ozemlju varuje človekove pravice in temeljne svoboščine (5. člen Ustave), mora v prvi vrsti skrbeti za obstoj in učinkovito delovanje institucij pravne države tudi tako, da se bori proti najhujšim oblikam kaznivih dejanj, da zagotavlja obrambo države in nacionalno varnost ter ustavno ureditev.

19. Zakonodajalec je torej za poseg v ustavno varovano pravico do informacijske zasebnosti iz prvega odstavka 38. člena Ustave imel ustavno dopustne cilje. S tega vidika poseg ni nedopusten.

20. Izpodbijani ukrep je tudi primeren za doseg navedenih ciljev, ker jih je s posegom dejansko mogoče doseči. Nedvomno sta v določenih primerih hramba in kasnejša uporaba prometnih podatkov lahko primeren način za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj. Prav tako za namene obrambe države in zaščito države varnosti. To izhaja tako iz izjav držav članic, kot je razvidno iz ocenjevalnega poročila Evropske komisije[17] in drugih dokumentov, objavljenih na njeni spletni strani,[18] kot tudi iz analize, ki jo je predložila Vlada v tem postopku. Vlada navaja, da imajo ti podatki pomembno podporno nalogo pri zbiranju dokazov v okviru preiskav kaznivih dejanj, saj kažejo na posamezna dejstva, okoliščine, relacije, dinamike in vzorce, ki pomembno pripomorejo k zbiranju temeljnih dokazov za neposredno dokazovanje suma storitve kaznivega dejanja. Tudi Sodišče Evropske unije je ocenilo, da so glede na vedno večji pomen sredstev elektronske komunikacije podatki, ki jih je bilo treba hraniti na podlagi neveljavne direktive, nacionalnim organom, pristojnim za kazenski pregon, omogočali dodatne možnosti za razkritje hudih kaznivih dejanj in so torej v zvezi s tem dragoceno sredstvo za kazenske preiskave.[19] Čeprav iz gradiva, ki ga je predložila Vlada, in iz dokumentov Komisije ni jasno razvidno, ali gre za uporabo podatkov, ki sicer ob odsotnosti obvezne hrambe, kot jo je predvidela Direktiva o hrambi podatkov in sedaj izpodbijana ureditev, ne bi bili dostopni organom pregona in drugim pristojnim državnim organom, pa hkrati tudi ni mogoče zaključiti, da bi bili ti podatki očitno neprimerni za doseg cilja. Prav tako ni očitno, da je ukrep neprimeren, tudi če je v določenih primerih zaradi tehničnih obvodov ali posebnih načinov uporabe teh storitev (npr. ponarejanje klicne številke, uporaba neregistriranih predplačniških mobilnih storitev, uporaba storitve za anonimizacijo prometa na internetu ipd.) mogoče zabrisati digitalne sledi za resničnim uporabnikom ali doseči anonimno uporabo mobilne in fiksne telefonije ter dostopa do interneta, na kar sicer opozarja predlagatelj. Ukrep je neprimeren šele takrat, kadar sredstvo za doseg cilja ni v razumni zvezi s tem ciljem in kadar s sredstvom navedenega cilja v nobenem primeru ni mogoče doseči, ne le zgolj v določenem obsegu.[20] Lahko pa to, da je z ukrepom mogoče doseči ustavno dopusten cilj le v določenem obsegu, pomembno vpliva na presojo sorazmernosti takega ukrepa.

21. Tudi če je ukrep lahko primeren in uporaben, to hkrati ne pomeni, da je nujno potreben oziroma da za uresničitev cilja, ki mu sledi, niso na voljo manj invazivni ukrepi, ki bi manj posegli v človekove pravice posameznikov.[21] V okviru preizkusa nujnosti posega Ustavno sodišče presoja, ali je poseg sploh nujen (potreben) v tem smislu, da cilja ni mogoče doseči brez posega nasploh (kateregakoli) oziroma da cilja ni mogoče doseči brez ocenjevanega (konkretnega) posega s kakšnim drugim, ki bi bil po svoji naravi blažji.[22]

22. Zato je treba oceniti, ali bi zakonodajalec namen, za katerega se je tak osebni podatek hranil, lahko dosegel tudi tako, da bi v pravico iz prvega odstavka 38. člena Ustave posegel na manj invaziven način. Glede na to, da je izpodbijana ureditev glede načina in obsega hrambe podatkov v bistvu prepis zahtev Direktive o hrambi podatkov in je torej določena na način, kot jo je določala sedaj razveljavljena Direktiva o hrambi podatkov, so razlogi, ki so Sodišče Evropske unije vodili pri njeni razveljavitvi, ključni tudi pri presoji izpodbijanega zakona.

23. V izhodišču je treba poudariti, da so boj proti hudim kaznivim dejanjem, še posebej organiziranemu kriminalu in terorizmu, obramba države in zagotavljanje nacionalne varnosti ter ustavne ureditve temeljnega pomena za delovanje pravne države. Vendar pa tak cilj, čeprav temeljnega pomena, sam po sebi ne more upravičevati neomejenega posega v človekove pravice.

24. Izpodbijana ureditev predvideva preventivno (vnaprejšnjo) in nediskriminacijsko hrambo prometnih podatkov določenih elektronskih komunikacij. Posledica takšne ureditve je, da operaterji hranijo določen čas prometne podatke vseh uporabnikov telefonskih storitev v fiksnem in mobilnem

omrežju, podatke pri dostopu do interneta, elektronske pošte in uporabe telefonije prek internetnega protokola, kot jih predvideva 164. člen ZEKom-1. Z vnaprejšnjo in neselektivno hrambo podatkov, ki nastajajo vsakodnevno, se pri operaterjih ustvarjajo ogromne podatkovne zbirke podatkov, ki se hranijo 14 oziroma 8 mesecev in iz katerih je mogoče v vsakem trenutku izluščiti zelo podrobna dejstva zasebnega življenja vsakega posameznika, ki uporablja te storitve.[23] Glede na to, da sodobni način komuniciranja pomeni v pretežni meri uporabo navedenih elektronskih komunikacijskih storitev,[24] tak ukrep v bistvu pomeni zelo invaziven poseg v (informacijsko) zasebnost celotne populacije, tako po obsegu oseb, ki jih ukrep zadeva, kot tudi glede na podatke, ki se hranijo. Poseg v pravico izostri tudi dejstvo, da se z nastankom tako obsežne zbirke osebnih podatkov celotne populacije izrazito poveča tveganje, da bodo do hranjenih podatkov kljub obveznostim, ki jih operaterjem med drugim nalaga 165. člen ZEKom-1, dostopale nepooblaščen osebe oziroma da se bodo podatki uporabili za nezakonite namene.[25] Taka ureditev izrazito posega v človekove pravice in temeljne svoboščine posameznika tudi zato, ker prizadete osebe o hrambi in morebitni kasnejši uporabi njihovih podatkov niso obveščene, kar lahko pri njih ustvari občutek stalnega nadzora.[26] Takšen neoprijemljiv občutek stalnega nadzora pa lahko vpliva tudi na izvrševanje drugih pravic, predvsem pravice do svobodnega izražanja in obveščanja, kot jo zagotavljata 39. člen Ustave in 11. člen Listine.[27]

25. Preventivna in neselektivna hramba podatkov po naravi stvari nujno pomeni, da posega v pretežni meri v pravice tistih, ki z nameni, zaradi katerih so bili v prvi vrsti ti podatki zbrani, nimajo oziroma ne bodo imeli niti posredne zveze. Tako kot Direktiva o hrambi podatkov tudi slovenski zakonodajalec ni hrambe zamejil na tiste podatke, ki so v neki razumni in objektivno preverljivi zvezi z namenom, ki ga ukrep želi doseči. Neselektivna in vnaprejšnja hramba prometnih podatkov nujno pomeni, da bo posegla v prevladujočem delu v pravice tistega dela populacije, ki ni dala povoda za takšen poseg. Kot je poudarilo tudi Sodišče Evropske unije,[28] se z nezamejenim ukrepom hranijo celo podatki o komunikacijah, ki bi sicer morale uživati še posebno zaščito. Ureditev namreč ne omogoča anonimne uporabe komunikacijskih sredstev za vse tiste primere, ko je zaupna in nesledljiva uporaba komunikacijskih sredstev nujna za doseg njenega namena (npr. telefonske storitve za pomoč v duševni stiski). Prav tako izpodbijana ureditev, tako kot tudi ne Direktiva o hrambi podatkov, ni zamejila hrambe podatkov na določeno časovno obdobje, geografsko območje ali krog oseb, ki bi lahko bili v določeni zvezi z namenom, ki ga ukrep zasleduje.[29]

26. Vprašanje časa hrambe osebnih podatkov je prav tako pomembno pri presoji, ali je ukrep nujen za doseg ustavno dopustnega cilja. Hramba oziroma obdelava osebnih podatkov dlje, kot je to še potrebno za doseg namena, ne zadosti sorazmernosti.[30] Zakonodajalec je sicer v petem odstavku 163. člena ZEKom-1 predvidel različen čas hrambe za podatke v zvezi z javno dostopnimi telefonskimi storitvami (14 mesecev) na eni strani in vse druge podatke na drugi strani (8 mesecev). Vendar pa razlogi, zakaj se je odločil za hrambo v tem časovnem obsegu in zakaj je določil različno dobo hrambe za navedene podatke, ne iz odgovora Državnega zbora ali mnenja Vlade in tudi ne iz zakonodajnega gradiva niso razvidni. V že omenjeni analizi, ki jo je priložila Vlada, je navedena le pavšalna ugotovitev, da bi v primeru skrajšanja roka hrambe "bila potrebna ponovna prilagoditev preiskovanih procesov". Glede na to, da se zbirajo različni podatki, ki imajo po naravi stvari različno uporabno vrednost glede na čas hrambe, bi zakonodajalec moral to upoštevati in čas hrambe ustrezno diferencirati glede na uporabnost podatkov ali glede na osebe, ki jih to zadeva.[31] Iz navedenega gradiva tudi ni razvidno, zakaj krajši rok hrambe (kot so ga npr. določile nekatere države članice)[32] ne zadostuje za doseg namena. Pri ukrepu, ki vključuje tako širok spekter različnih podatkov, ne da bi bila natančneje določena objektivna merila za takšno hrambo, tudi ni mogoč kasnejši preizkus, ali se ukrep nanaša le na to, kar je še nujno potrebno za doseg namena. Takšen ukrep ne zadosti merilu nujnosti in tudi ne merilu sorazmernosti v ožjem pomenu, ker ni mogoče pretehtati, ali je ustrezno daljša doba hrambe in s tem povezana stopnja posega v zasebnost posameznika sorazmerna z

zagotavljanjem javne varnosti oziroma drugega interesa, ki mu ukrep sledi.

27. Že razveljavljena Direktiva o hrambi podatkov je namen hrambe omejila le za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj. Izpodbijana ureditev takšne omejitve ne vsebuje. Zakonodajalec tudi v predpisih, na katere se izpodbijana ureditev sklicuje (prvi odstavek 163. člena ZEKom-1), obdelave prometnih podatkov ni zamejil zgolj na določena (huda kazniva) dejanja, za katera bi ocenil, da zaradi njihove teže hramba podatkov oziroma dostop do njih upravičujeta poseg v zasebnost posameznika.[33] Tudi zato ukrep nesorazmerno posega v pravico iz prvega odstavka 38. člena Ustave.

28. Zakonodajalec je z določitvijo obvezne hrambe prometnih podatkov v prvem odstavku 163. člena ZEKom-1 izrazilo posegel v pravico do varstva osebnih podatkov, hkrati pa ni skrbno opredelil okoliščin, na podlagi katerih bi ta poseg zamejil le na tisto, kar je še nujno potrebno za doseg namena. S tem je izpodbijana določba nesorazmerno posegla v pravico do varstva osebnih podatkov iz prvega odstavka 38. člena Ustave. Zato je prvi odstavek 163. člena ZEKom-1, ki izrecno določa obvezno hrambo prometnih podatkov, protiustaven. Druge izpodbijane določbe XIII. poglavja ZEKom-1 pa so neposredno s to določbo povezane in nimajo samostojnega pomena. Zato je Ustavno sodišče izpodbijane določbe XIII. poglavja razveljavilo v celoti (1. točka izreka).

29. Ker je bilo treba izpodbijane določbe razveljaviti že zaradi neskladja s pravico do varstva osebnih podatkov po 38. členu Ustave, Ustavno sodišče ni presojalo drugih zatrjevanih protiustavnosti.

30. Da bi Ustavno sodišče preprečilo nadaljnje nesorazmerne posege v pravico do varstva osebnih podatkov iz prvega odstavka 38. člena Ustave, je na podlagi drugega odstavka 40. člena ZUstS določilo način izvršitve te odločbe. Na njegovi podlagi morajo operaterji, ki hranijo prometne podatke po prvem odstavku 163. člena ZEKom-1, nemudoma po objavi te odločbe v Uradnem listu Republike Slovenije te podatke uničiti (2. točka izreka).

C.

31. Ustavno sodišče je sprejelo to odločbo na podlagi 43. člena in drugega odstavka 40. člena ZUstS v sestavi: predsednik mag. Miroslav Mozetič ter sodnice in sodniki dr. Mitja Deisinger, dr. Dunja Jadek Pensa, dr. Etelka Korpič – Horvat, dr. Ernest Petrič, Jasna Pogačar, dr. Jadranka Sovdat in Jan Zobec. Ustavno sodišče je odločbo sprejelo soglasno.

mag. Miroslav Mozetič
Predsednik

Opombe:

[1] To izhaja iz vsebine zakonskih določb in še posebej iz drugega odstavka 2. člena ZEKom-1 ter iz namena zakonodajalca, izraženega v predlogu zakona (Poročevalec DZ z dne 1. 10. 2012, EPA 667-VI).

[2] Poročilo Komisije Svetu in Evropskemu parlamentu, Ocenjevalno poročilo o Direktivi o hrambi podatkov (Direktiva 2006/24/ES) z dne 18. 4. 2011, COM (2011) 225 konč.

[3] Glej obrazložitev k XIII. poglavju ZEKom-1 (Hramba podatkov) v predlogu zakona (Poročevalec DZ z dne 1. 10. 2012) "[...] Z vidika jasnosti ureditve, saj gre za prenos dveh različnih direktiv (Direktiva o

zasebnosti in elektronskih komunikacijah ter Direktiva o hrambi podatkov), se v ZEKom-1 uvaja novo poglavje, ki se nanaša le na prenos Direktive o hrambi podatkov, kot je to bilo sicer že zagotovljeno v sklopu X. poglavja ('Zaščita tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hramba podatkov o prometu elektronskih komunikacij') obstoječega ZEKom. [...]"

[4] Glej 92. člen ZEKom-A, ki je vnesel nov 107.a do 107.e člen.

[5] Peti odstavek 163. člena ZEKom-1.

[6] Prim. odločbo Ustavnega sodišča št. U-I-18/02 z dne 24. 10. 2003 (Uradni list RS, št. 108/03, in OdlUS XII, 86).

[7] Glej npr. mnenje Delovne skupine za varstvo podatkov iz 29. člena o definiciji osebnih podatkov iz leta 2007.

[8] Glej sodbo v združenih zadevah *Volker und Markus Schecke GbR in Hartmut Eifert proti zvezni deželi Hessen*, C-92/09 in C-93/09, z dne 9. 11. 2010.

[9] Glej drugi stavek 29. točke sodbe v združenih zadevah C-293/12 in C-594/12.

[10] Glej predvsem sodbe Evropskega sodišča za človekove pravice (v nadaljevanju ESČP) v zadevah *Leander proti Švedski* z dne 26. 3. 1987, *Amann proti Švici* z dne 16. 2. 2000, *Kopp proti Švici* z dne 25. 3. 1998.

[11] Glej 12. točko obrazložitve odločbe Ustavnega sodišča št. U-I-98/11 z dne 26. 9. 2012 (Uradni list RS, št. 79/12).

[12] Prim. odločbo Ustavnega sodišča št. U-I-18/02.

[13] Tako že v odločbi št. U-I-411/06 z dne 19. 6. 2008 (Uradni list RS, št. 68/08, in OdlUS XVII, 43).

[14] Glej odločbo št. U-I-312/11 z dne 13. 2. 2014 (Uradni list RS, št. 15/14).

[15] Tako npr. že v odločbi št. U-I-98/11.

[16] Glej tudi uvodne izjave 4, 5 in od 7 do 11 ter 21 in 22 Direktive o hrambi podatkov.

[17] Poročilo Komisije Svetu in Evropskemu parlamentu, Ocenjevalno poročilo o Direktivi o hrambi podatkov (Direktiva 2006/24/ES) z dne 18. 4. 2011.

[18] Glej npr. *Evidence for necessity of data retention in the EU* dostopno na ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf (2. 7. 2014).

[19] Točka 49 obrazložitve sodbe v združenih zadevah C-293/12 in C-594/12.

[20] Glej odločbo št. U-I-201/93 z dne 7. 3. 1996 (Uradni list RS, št. 24/96, in OdlUS V, 27). Primerjaj tudi z 207. točko obrazložitve sodbe Zveznega ustavnega sodišča Zvezne republike Nemčije št. 1 BvR 2156/08, 1 BvR 263/08, 1 BvR 586/08 z dne 2. 3. 2010.

[21] ESČP v okviru presoje sorazmernosti ukrepa (oziroma nujnosti ukrepa v demokratični družbi) poudarja, da pridevnik "nujen" ni sopomenka za "neobhodno potreben", hkrati pa ga tudi ni mogoče razlagati tako prožno kot na primer izraze "dopusten", "reden", "koristen", "razumen" ali "zaželen" (sodba v zadevi *Handyside proti Združenemu kraljestvu* z dne 7. 12. 1976).

[22] Tako npr. v odločbi št. U-I-77/08 z dne 8. 7. 2010 (Uradni list RS, št. 61/10).

[23] Glej 14. točko obrazložitve.

[24] Glej 72. in 73. točko sklepnih predlogov generalnega pravobranilca Pedra Cruza Villalona z dne 12. 12. 2013 v združenih zadevah C-293/12 in C-594/12 in sodbe ESČP, na katere se sklicuje.

[25] Prav tam, 75. točka.

[26] Operater dejstva, da je do posredovanja podatkov prišlo, namreč ne sme razkriti osebi, na katero se podatki nanašajo (četrti odstavek 166. člena ZEKom-1).

[27] Tako že sodba Zveznega ustavnega sodišča Zvezne republike Nemčije št. 1 BvR 2156/08, 1 BvR 263/08, 1 BvR 586/08 in 37. točka obrazložitve sodbe v združenih zadevah C-293/12 in C-594/12.

[28] Glej 58. točko obrazložitve sodbe v združenih zadevah C-293/12 in C-594/12.

[29] Prav tam, 59. točka.

[30] Odločba Ustavnega sodišča št. U-I-312/11 z dne 13. 2. 2014 (Uradni list RS, št. 15/14). Glej tudi sodbo ESČP v zadevi *S. in Marper proti Združenemu kraljestvu* z dne 4. 12. 2008. Tako tudi 6. člen Direktive o zasebnosti in elektronskih komunikacijah in točka e) 5. člena MKVP. Glej tudi 24. točko obrazložitve v odločbi št. U-I-411/06. Člen 6 Direktive o zasebnosti in elektronskih komunikacijah

določa načelo, da je treba podatke o prometu, ki se obdelujejo, izbrisati ali anonimizirati, potem ko niso več potrebni za namen prenosa sporočila.

[31] Primerjaj s 63. in 64. točko sodbe v združenih zadevah C-293/12 in C-594/12.

[32] Npr. šestmesečni rok, kot ga je določila Zvezna republika Nemčija v (sedaj sicer razveljavljenem) 113.a členu Zakona o telekomunikacijah (*Telekommunikationengesetz*).

[33] Primerjaj prvi odstavek 149.b člena Zakona o kazenskem postopku (Uradni list RS, št. 32/12 – uradno prečiščeno besedilo in 47/13 – v nadaljevanju ZKP) in drugi odstavek 150. člena ZKP, kjer je zakonodajalec določil katalog kaznivih dejanj, v zvezi s katerimi se lahko odredijo ukrepi iz prvega odstavka 150. člena ZKP.

Vrsta zadeve:

ocena ustavnosti in zakonitosti predpisov in drugih splošnih aktov

Vrsta akta:

zakon

Vlagatelj:

Informacijski pooblaščenec, Ljubljana

Datum vloge:

6. 3. 2013

Datum odločitve:

3. 7. 2014

Vrsta odločitve:

odločba

Vrsta rešitve:

razveljavitev ali odprava

Objava:

Uradni list RS, št. 54/2014 in OdlUS XX, 27

Dokument:

US30439