INFORMACIJSKI POOBLAŠČENEC
Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si
REPUBLIKA SLOVENIJA

Številka:
Datum:

USTAVNO SODIŠČE REPUBLIKE SLOVENIJE
Beethovnova 10
1000 Ljubljana, p.p. 1713

Informacijski pooblaščenec na podlagi 6. alineje 1. odstavka 23.a člena Zakona o ustavnem sodišču (Ur. l. RS, št. 64/2007-UPB1, 108/2007 Skl.US: U-I-259/07-10; ZUstS) vlaga v zvezi z zadevo inšpekcijskega nadzora pod št. 0613-18/2013 naslednjo

ZAHTEVO ZA OCENO USTAVNOSTI IN ZAKONITOSTI

XIII. poglavja (hramba podatkov) - členov 162, 163, 164, 165, 166, 167, 168 in 169 Zakona o elektronskih komunikacijah (Uradni list RS, št. 109/2012; ZEKom-1).

in

PREDLOG ZA ABSOLUTNO PREDNOSTNO OBRAVNAVO ZADEVE

in

PREDLOG ZA ZAČASNO ZADRŽANJE IZVRŠEVANJA IZPODBIJANIH DOLOČB ZEKOM-1

Utemeljitev obstoja procesne predpostavke

Na podlagi šeste alineje prvega odstavka 23.a člena ZUstS lahko Informacijski pooblaščenec (v nadaljevanju: Pooblaščenec ali vlagatelj) z zahtevo začne postopek za oceno ustavnosti oziroma zakonitosti predpisa, če nastane vprašanje ustavnosti ali zakonitosti v zvezi s postopkom, ki ga vodi. Vlagatelj pod številko 0613-18/2013 vodi postopek inšpekcijskega nadzora nad ravnanjem zavezanca Si.mobil d.d., Šmartinska cesta 134b, 1000 Ljubljana - glede zakonitosti izvajanja določb ZEKom-1 o obvezni hrambi podatkov o prometu elektronskih komunikacij. V okviru inšpekcije je bilo ugotovljeno, da se v zbirko podatkov, ki se obvezno hranijo, pri zavezancu vsak dan vključi več milijonov novih podatkov (podatkov o klicih, SMS/ MMS sporočil, sporočilih elektronske pošte, podatkov o vzpostavljenih sejah za dostop do interneta …). To pomeni, da je zbirka obvezno hranjenih podatkov vsak dan »bogatejša« za več milijonov osebnih podatkov, ki se nanašajo na posameznike - uporabnike storitev zavezanca. Zavezanec torej za potrebe države (in ne za potrebe izvajanja pogodbe o zagotavljanju storitev) vsak dan shrani več milijonov osebnih podatkov in jih v odvisnosti od tega, ali gre za podatke o javno dostopni telefonski storitvi ali za druge podatke, hrani še 14 oziroma 8 mesecev. Po določbah ZEKom-1 se podatki obvezno hranijo za namene kazenskega postopka, za namene zagotavljanja nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države – torej izključno za potrebe države. Pooblaščenec je ob inšpekcijskem ogledu tudi ugotovil, da je zavezanec v letu 2009 prejel 373

sodnih odredb za posredovanje podatkov, ki se hranijo, v letu 2010 688 odredb, v letu 2011 692 odredb in v letu 2012 583 odredb.

Pooblaščenec je torej v inšpekcijskem postopku št. 0613-18/2013 ugotovil, da zgolj zavezanec Si.mobil d.d. v zbirko podatkov, ki se obvezno hranijo, na dan shrani več milijonov osebnih podatkov svojih uporabnikov – na leto torej več sto milijonov osebnih podatkov, med tem ko prejme letno (le) med 400 in 700 sodnih odredb za njihovo posredovanje. Očitno je torej, da so osebni podatki enormne večine uporabnikov elektronskih komunikacij obdelovani zgolj »za vsak slučaj«, in ne operaterju (zavezancu) ne državi niso resnično potrebni. Shranjujejo se zgolj zaradi peščice primerov, v katerih je izdana sodna odredba. Ta izjemen razkorak med količino shranjenih in dejansko zahtevanih (potrebnih) osebnih podatkov po prepričanju Pooblaščenca neposredno kaže na očitno nesorazmernost zakonske ureditve, ki grobo posega v komunikacijsko in informacijsko zasebnost slehernega uporabnika elektronskih komunikacijskih sredstev zaradi potencialne uporabnosti podatkov za nacionalno varnost in kazenski postopek.

Pooblaščenec meni, da v opisanih okoliščinah posameznikom, katerih osebni podatki se obvezno hranijo po določbah ZEKom-1, s pooblastili, ki so mu poverjena, glede na določila XIII. poglavja ZEKom-1 ne more zagotoviti učinkovitega varstva informacijske zasebnosti (38. člen Ustave RS), zato vlaga na Ustavno sodišče pričujočo zahtevo za oceno ustavnosti sporne zakonske ureditve.

Predlog za absolutno prednostno obravnavo zadeve

Po drugi alineji tretjega odstavka 46. člena Poslovnika Ustavnega sodišča Ustavno sodišče lahko sklene, da bo kot prednostno obravnavalo zadevo, v kateri gre za reševanje pomembnega pravnega vprašanja.

Vlagatelj poudarja, da gre pri izpodbijanih določbah za pomembno pravno vprašanje zaradi dileme o tem:

- ali so določbe ZEKom-1 v skladu z načelom pravne države (načelom sorazmernosti), saj se učinek zatrjevane neustavnosti, ki se kaže v posegih v temeljne človekove pravice, razteza na celotno populacijo oziroma na vse posameznike, ki so »ujeti« pri komunikaciji prek baznih postaj operaterjev, ki imajo sedež v Republiki Sloveniji;
- ali je *Direktiva 2006/24/ES 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* (v nadaljevanju: Direktiva) v ZEKom prenesena pravilno; v skladu s cilji Direktive, neposredno in popolnoma.

Kadar domnevna neustavnost posega v pravice slehernika, ne da bi ta oblasti dal kakršenkoli povod, ki bi poseg dovoljeval (torej zgolj zaradi dejstva komunikacije prek elektronskih komunikacijskih sredstev), gre po mnenju vlagatelja za tako pomembno pravno vprašanje, ki terja prednostno obravnavo. Enako predlagatelj meni glede vprašanja pravilnosti prenosa Direktive. Slednje ni le pomembno pravno vprašanje, ki vpliva na nacionalno pravo, temveč gre tudi ali predvsem za spoštovanje prava EU.

1) Vprašanje sorazmernosti obvezne hrambe podatkov.

Zatrjujoč kršitve določenih pravic in svoboščin posameznikov, predvsem pa očitno nesorazmernost ukrepa obvezne hrambe so Ustavna sodišča Nemčije[1], Romunije[2], Češke[3] in Višje sodišče Irske[4], že prepoznala ukrep kot sporen. Tudi Ustavno sodišče Republike Avstrije je zaradi dvomov o skladnosti Direktive z Evropsko konvencijo o temeljnih pravicah in svoboščinah v decembru 2012 na Sodišče EU naslovilo zahtevo za predhodno odločanje[5].

Pomisleki o nesorazmernosti ukrepa izhajajo iz dejstva, da ta zadeva in prizadene slehernega, ki uporablja pri komunikaciji elektronska komunikacijska sredstva, ne glede na to, da se v celoti ravna po pravu in ne krši nobenega prepisa.

Po drugem odstavku 38. člena Ustave RS zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Tudi ustavno podprto predpisovanje načina uresničevanja človekove pravice (tokrat do varstva osebnih podatkov, tajnosti pisanj, svobode gibanja) pa mora prestati test sorazmernosti. O tem se je Ustavno sodišče opredelilo že v številnih odločbah. *Vsebinska skladnost zakona z ustavo mora biti v skladu, ne samo s posameznimi posebnimi ustavnimi določbami, ampak tudi s temeljnimi vrednotami svobodne*

[1] Povzetek odločbe Ustavnega sodišča R Nemčije:
http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional
[2] Povzetek odločbe Ustavnega sodišča R Romunije:
http://www.edri.org/edrigram/number7.23/romania-decision-data-retention
[3] Povzetek odločbe Ustavnega sodišča R Češke:
http://www.edri.org/czech-decision-data-retention
[4] Povzetek odločbe Višjega sodišča (High Court) R Irske:
http://www.digitalrights.ie/2010/05/05/high-court-decision-on-our-data-retention-challenge/
[5] Več o zahtevi ustavnega sodišča R Avstrije je dosegljivo na povezavi: http://www.vfgh.gv.at/

demokratične ustavne ureditve kot ustavnopravne vrednostne kategorije[6]. Tako je bilo tudi prepoved čezmernih posegov države oz. načelo sorazmernosti z odločitvami Ustavnega sodišča postavljeno na raven ustavnega načela, ki zavezuje vse državne organe, začenši z zakonodajalcem, ne le pri sprejemanju splošnih pravnih predpisov, ampak tudi pri njihovem izvrševanju.

Pooblaščenec tako zatrjuje, da je pri izpodbijani zakonski ureditvi podatkov, ki se obvezno hranijo, sicer spoštovano legalitetno načelo, povsem spregledano pa je bilo načelo sorazmernosti. Zakonodajalec je torej urejal obdelavo osebnih podatkov na način, ki ni skladen s pravno državo, saj ni spoštoval lastnih omejitev pri urejanju posegov v človekove pravice. Z absolutističnim pristopom k regulaciji podatkov, ki se hranijo, pa je posegel tudi v pravice posameznikov, ki se nanašajo na tajnost pisanj, svobodo izražanja in svobodo gibanja in to na način oziroma z intenziteto, ki se na drugi strani ne odraža v boljši raziskanosti (hujših) kaznivih dejanj. Raziskava Delovne skupine za hrambo podatkov[7] ugotavlja, da ima splošna hramba podatkov lahko celo negativen učinek na raziskanost kaznivih dejanj. Da bi se izognili hrambi osebnih podatkov, kot jo določa zakon, se posamezniki zatekajo h komunikaciji v internetnih kavarnah, prek brezžičnih internetnih dostopnih točk, anonimnih storitev, javnih telefonov, predplačniških - neregistriranih SIM kartic, pa tudi (znova) k uporabi ne-elektronske komunikacije. Takšno vedenje pa ne le, da hrambo podatkov po ZEKom-1 dela nesmiselno, ampak ima širše neželene učinke – v oteževanju oziroma celo onemogočanju uspešnega izvajanja tudi klasičnih zakonitih usmerjenih preiskovalnih tehnik (npr. prisluškovanja kot prikritega ukrepa). Tako lahko zavedanje posameznikov o obstoju in obsegu obvezne hrambe podatkov prav zaradi intenzivnosti njegovega posega v vrsto človekovih pravic pripelje v končnem rezultatu do zmanjšanja možnosti za uspešno preiskavo kaznivih dejanj. In ko na koncu kot rezultat ostane le poseg v človekove pravice (negativna komponenta ukrepa) brez protiuteži v močni javni koristi, ki bi se kazala v (bistveno) povečani raziskanosti (hudih) kaznivih dejanj (pozitivna komponenta ukrepa), bi morala biti ugotovitev o očitni nesorazmernosti posega in njegovih posledic očitna in enostavna – ukrep obvezne hrambe podatkov ni sorazmeren z njegovimi posledicami in je posledično protiustaven.

Podrobnejšo utemeljitev trditve, da je bilo pri izpodbijani zakonodajni ureditvi povsem spregledano ravnotežje med pričakovanim rezultatom in prizadetostjo pravic posameznikov Pooblaščenec podaja v točki III) te zahteve.

Na ta način je po mnenju vlagateljev kršen 2. člen v povezavi z 32., 35., 37., 38. in 39. členom Ustave RS.

2) Vprašanje pravilnosti prenosa Direktive v ZEKom-1.

Vlagatelj zatrjuje, da je zakonodajalec hrambo podatkov v izpodbijanih členih prenesel v nasprotju z nameni Direktive.

Direktiva v 1/I. členu določa:
Namen te direktive je uskladiti določbe držav članic glede obveznosti ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij glede hrambe določenih podatkov, ki jih pridobivajo

[6] Citat iz Komentarja ustave Republike Slovenije: Fakulteta za podiplomske državne in evropske študije, 2002; str. 53.
[7] Dosegljiva na povezavi: http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

ali obdelujejo, da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic.

Namen Direktive je bil resda v vzpostavitvi obveznosti hrambe določenih podatkov, ki jih (tudi sicer za namen zagotavljanja javno dostopne komunikacijske storitve in za čas do izpolnitve tega namena) obdelujejo operaterji, vendar naj bi se posegi države v tako shranjene podatke omejili le na *namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic.* Nameni hrambe podatkov po ZEKom-1 pa močno odstopajo od zamišljene enotne ureditve v EU.
Prvi odstavek 163. člena tako določa, da se podatki hranijo:

- 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 namene obrambe države, kakor jih določa zakon, ki ureja obrambo države.

ZEKom-1 (pred njim tudi ZEKom – Uradni list RS, št. 43/2004 s spremembami in dopolnitvami) je hranjene podatke o komunikaciji prek elektronskih sredstev namesto preprečevanju, preiskovanju, odkrivanju in pregonu hudih kaznivih dejanj, namenil za kakršnokoli pridobivanje osebnih podatkov po zakonih, ki urejajo kazenski postopek, Slovensko obveščevalno-varnostno agencijo in obrambo države. Takšna ureditev je vsekakor v nasprotju s cilji Direktive. Kot vsaka direktiva je tudi Direktiva namenjena usklajevanju pravnih ureditev držav članic - tokrat na področju obvezne hrambe podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij. Cilj takšne usklajenosti pa je zagotavljanje enakih pravic in obveznosti vsem pravnim in fizičnim osebam na območju Evropske unije. Direktiva mora biti prenesena neposredno in popolnoma. V primeru prenosa Direktive ni bilo tako. Posledično se pravice in obveznosti pravnih in fizičnih oseb, ko te uporabljajo omrežja in storitve slovenskih ponudnikov javno dostopnih komunikacijskih in omrežij (operaterjev), razlikujejo od pravic, ki jih osebe uživajo v drugih državah (tudi) članicah EU.

Na ta način je po mnenju vlagatelja kršen 3.a/III člen Ustave RS.

Predlog za začasno zadržanje izvrševanja izpodbijanih določb ZEKom-1

Po določbi 39. člena Zakona o ustavnem sodišču (Uradni list RS, št. 64/2007 – UPB1; v nadaljevanju: ZUstS) sme Ustavno sodišče do končne odločitve v celoti ali delno zadržati izvršitev predpisa ali splošnega akta za izvrševanje javnih pooblastil, če bi zaradi njegovega izvrševanja lahko nastale težko popravljive škodljive posledice.

Vlagatelj zahteve predlaga Ustavnemu sodišču, da do dokončne odločitve zadrži izvajanje izpodbijanih določb ZEKom-1.

Kadar Ustavno sodišče odloča o začasnem zadržanju izvrševanja izpodbijanega predpisa, vselej tehta med škodljivimi posledicami, ki bi jih povzročilo izvrševanje protiustavnega predpisa, in škodljivimi posledicami, ki bi nastale, če se izpodbijane določbe sploh ne bi izvrševale. Škodljive posledice, ki bi nastale z izvrševanjem izpodbijanih določb, morajo biti po presoji Ustavnega sodišča hujše od posledic, ki jih lahko povzroči začasno zadržanje njihovega izvrševanja, če bi se izkazale za protiustavne.

Podatki, ki se hranijo po izpodbijanih določbah ZEKom-1, so podatki o prometu in lokaciji ter z njimi povezani podatki, ki določajo naročnika ali uporabnika javne komunikacijske storitve. Ti podatki se shranijo o slehernem telefonskem klicu, vključno z govornimi klici, govorno pošto, konferenčnimi ali podatkovnimi klici, dopolnilnimi storitvami, vključno s preusmeritvijo in predajo klica, pošiljanjem sporočil in multimedijskimi storitvami, vključno s storitvijo kratkih sporočil, nadgrajenimi medijskimi storitvami in multimedijskimi storitvami. Prav tako se ti podatki shranijo o slehernem dostopu do interneta, elektronske pošte in uporabi telefonije prek internetnega protokola.

Cilj hrambe podatkov je bil v boljši raziskanosti (hujših) kaznivih dejanj. Sorazmernost med pričakovanim učinkom in posegi v pravice vsakogar bi bila torej podana, če bi se raziskanost (hujših) kaznivih dejanj po uvedbi obvezne hrambe podatkov resnično (bistveno) povečala. Pomembno višja stopnja raziskanosti (hujših) kaznivih dejanj bi lahko opravičila prevlado javnega interesa, ki je v učinkih generalne in specialne prevencije, nad interesi slehernega posameznika, da uživa zasebnost, se svobodno (nenadzorovano) giblje, komunicira, izraža mnenja ipd.

Po štirih oziroma šestih[8] letih od uvedbe obvezne hrambe je jasno, da se raziskanost kaznivih dejanj, zaradi obvezne hrambe podatkov, ni povečala. Policijska statistika je sicer zelo skopa (kar je problem, ki govori sam zase). Zadnja dosegljiva priča o tem, da je bilo v letu 2008 po prvem odstavku 149.b člena izvedenih 1580 ukrepov, 264 zahtev policije pa je preiskovalni sodnik zavrnil. V letu 2009 je bilo izvedenih 1271 ukrepov po prvem odstavku 149.b člena ZKP, preiskovalni sodnik pa jih je zavrnil 365[9]. Žal starejših ali novejših podatkov ni, predvsem pa ni podatkov o končnem uspehu v konkretnem kazenskem postopku; je bil osumljenec na podlagi pridobljenih podatkov, ki se hranijo, obsojen ali oproščen. Bolj zgovorni so primerljivi podatki iz raziskave nemškega Inštituta Max Planck za tuje in mednarodno kazensko pravo[10]. Študijo je naročilo nemško pravosodno ministrstvo. V njej so ugotovili, da ukrepi hranjenja prometnih podatkov ne pripomorejo k večji raziskanosti ali preventivi pred kriminalnimi dejanji, zato niso smiselni[11]. Pomanjkanje empiričnih podatkov o

[8] ZEKom-A (Uradni list RS, št. 129/06) je v 121. členu določal: Določbe 92. člena tega zakona, ki se nanašajo na hrambo podatkov pri telefonskih storitvah, se začnejo uporabljati 15. septembra 2007, določbe, ki se nanašajo na hrambo podatkov o dostopu do interneta, elektronski pošti in internetni telefoniji, pa 15. marca 2009.
[9] Vir: https://slo-tech.com/novice/t470512
[10] http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile
[11] Kratek povzetek dosegljiv v članku na povezavi: https://slo-tech.com/novice/t504584

koristnosti pridobitve podatkov, ki se hranijo, v kazenskih postopkih, sicer ne omogoča povsem očitnih in kategoričnih zaključkov, ki pa, če gre za vprašanje spoštovanja načela sorazmernosti, niti niso potrebni. Seveda gre pomanjkanje podatkov na videz v korist zagovornikov obvezne in splošne hrambe, vendar bi moralo pravzaprav prav njim iti v škodo. Država (oblast) je namreč tista, ki bi morala dokazati (vedno znova dokazovati), da je obvezna hramba podatkov ključna za višjo stopnjo raziskanosti kaznivih dejanj ali/in za zmanjšanje števila kaznivih dejanj zaradi preventivnega učinka hrambe podatkov. Če tega z empiričnimi podatki ni sposobna dokazati (in podatki niso na voljo, ker ne čuti te potrebe, ali ker ji ne pričajo v korist), bi morala biti obvezna hramba že v izhodišču prepoznana kot prekomeren ukrep. V tem primeru obvezna hramba podatkov ne le, da ne dosega želenega cilja v meri, ki bi morebiti odtehtal posege v človekove pravice posameznikov, ki se z ničemer niso »pregrešili« zoper pravni red, ampak cilja sploh ne dosega. Po štirih oziroma šestih letih obvezne hrambe podatkov smo glede na navedeno lahko prepričani, da je Slovenija primer države, kjer obvezna hramba ne pripomore k višji raziskanosti kaznivih dejanj ali k njihovi preprečitvi. Na izrecno zaprosilo Pooblaščenca po posredovanju analize uporabe podatkov v prometu elektronskih komunikacij, je slovenska policija zapisala, da operativnih analiz zaradi njihove stroge namenskosti Pooblaščencu ne more posredovati, da pa je »končni doprinos podatkov in analiz vezan na edinstvene okoliščine vsakega posameznega kaznivega dejanja in je zato izrazito singularen in neprimerljiv«. Kot odmevne primere, v katerih so imeli podatki v prometu elektronskih komunikacij vidnejšo vlogo pri dokazovanju okoliščin, pa so izpostavili: trojni umor na Gorjancih leta 2003, trojni umor v Rovinju leta 2002, dvojni umor v Dobruški vasi in poskus umora v Brezju leta 2005 – torej vse pred zapovedano obvezno hrambo podatkov[12]. Očitno torej cilj regulacije ni dosežen, saj ni najti argumentov, da bi prav obvezna hramba pripomogla k večji raziskanosti (hujših) kaznivih dejanj.

Na drugi strani ni dvoma, da obvezna hramba podatkov o prometu in lokaciji ter z njimi povezanih podatkov, ki določajo naročnika ali uporabnika javne komunikacijske storitve, posega v več človekovih pravic. Nemški Inštitut za raziskovanje javnega mnenja Forsa je že v letu 2008 opravil raziskavo vpliva obvezne hrambe podatkov na vedenje posameznikov[13]. Raziskava je pokazala, da so (bi) ljudje zaradi obvezne hrambe prometnih podatkov spremenili svoje telekomunikacijske navade. Izsledki raziskave so pokazali, da je za obvezno hrambo prometnih podatkov slišalo 73% anketiranih, dobra desetina (11%) pa jih je izjavila, da zaradi ukrepa obvezne hrambe prometnih podatkov v določenih okoliščinah že niso uporabili telefona ali e-pošte. Šest odstotkov anketirancev je bilo prepričanih, da so zaradi tega ukrepa prejeli manj klicev in e-sporočil, dobra polovica (52%) pa jih je izjavila, da zaradi hrambe podatkov telekomunikacijskih sredstev verjetno ne bi uporabili za pogovor s farmacevtom (glede uživanja zdravil), psihoterapevtom ali ženitnim svetovalcem[14].

Obvezna hramba podatkov torej vpliva na posameznikovo dojemanje svobode/represivnosti oblasti; posega v njegovo pravico do svobode gibanja, zasebnosti, tajnosti pisanj, varstva osebnih podatkov in svobodo izražanja. Podatki o prometu in lokaciji ter z njimi povezani podatki o naročniku ali uporabniku javne komunikacijske storitve se namreč ne obdelujejo zgolj zaradi posameznikovega naročila operaterju, da opravi določeno storitev in v obsegu, ki je potreben za opravo storitve. Podatki se štirinajst mesecev[15] hranijo samo za državo – za njen represivni aparat; policijo, Slovensko varnostno obveščevalno agencijo in obveščevalno varnostno službo Ministrstva za obrambo. Še več – hranijo se za vsak primer… Gre namreč za podatke, ki jih nobena demokratična država v resnici ne potrebuje. V določenih primerih naj bi ti podatki olajšali iskanje osumljencev storitve kaznivih dejanj (v Sloveniji ne le teh, ampak tudi *»tistih, ki ogrožajo nacionalno varnost, ustavno ureditev, varnostne, politične in gospodarske interese države ter obrambo države«* - kot jih prepoznata

[12] Glej dopis Policije št. 092-95/2012/2 (224-09) z dne 4.2.2013 (v priloženem spisu).
[13] http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf
[14] Povzeto po članku: https://slo-tech.com/novice/t315344
[15] … in osem mesecev, če gre za podatke o dostopu do interneta, elektronske pošte in uporabi telefonije prek internetnega protokola.

varnostno obveščevalni službi), vendar gre pri tem argumentu pretežno za politično privlačno hipotetično izhodišče (izgovor), pri čemer pa je poseg v človekove pravice velike večine konformnih posameznikov realno dejstvo. Ta poseg se ponavlja s hrambo vsakega novega podatka in je po prepričanju vlagatelja zahteve v očitnem nesorazmerju z doseženimi cilji obvezne hrambe.

Ker so z uvedbo obvezne hrambe podatkov o prometu in lokaciji ter z njimi povezanih podatkov, ki določajo naročnika ali uporabnika javne komunikacijske storitve (že) nastale škodljive posledice, ki se kažejo v posegih v temeljne človekove pravice množice posameznikov in z vsakim novim shranjenim podatkom še vedno nastajajo, Pooblaščenec predlaga, da Ustavno sodišče do odločitve o zahtevi za oceno ustavnosti izpodbijanih določb ZEKom zadrži njihovo izvajanje. Neizvrševanje izpodbijanih določb na drugi strani po prepričanju vlagatelja ne bo imelo posledic na raziskanost kaznivih dejanj ali na povečanje števila kaznivih dejanj. Podrobnejši argumenti so navedeni v sami zahtevi, že samo dejstvo, da podatkov o tem, da se je povečala raziskanost kaznivih dejanj in/ali zmanjšalo njihovo število, sploh ni, pa priča o tem, da se država (oblast) z učinki obvezne hrambe podatkov ne more ravno pohvaliti.

(I) Izpodbijane določbe ZEKom-1

XIII. HRAMBA PODATKOV

162. člen

(pomen izrazov)

Ne glede na določbo 3. člena tega zakona imajo izrazi, uporabljeni v tem poglavju, naslednji pomen:

1. Podatki pomenijo podatke o prometu in lokaciji ter povezane podatke, potrebne za določitev naročnika ali uporabnika.

2. Uporabnik je pravna ali fizična oseba, ki uporablja javno komunikacijsko storitev v zasebne ali poslovne namene, čeprav ni nujno, da je naročena nanjo.

3. Telefonska storitev pomeni klice, vključno z govornimi klici, govorno pošto, konferenčnimi ali podatkovnimi klici, dopolnilne storitve, vključno s preusmeritvijo in predajo klica, pošiljanje sporočil in multimedijske storitve, vključno s storitvijo kratkih sporočil, nadgrajene medijske storitve in multimedijske storitve.

163. člen

(splošne določbe o podatkih, ki se hranijo)

(1) Operater mora 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.

(2) Obveznost iz prejšnjega odstavka ima operater, ki pridobiva ali obdeluje podatke iz 164. člena tega zakona in je sedež družbe ali podružnice oziroma oprema za izvajanje javne komunikacijske storitve ali za zagotavljanje javnega komunikacijskega omrežja v Republiki Sloveniji.

(3) Obveznost iz prvega odstavka tega člena vključuje tudi hrambo podatkov iz 164. člena tega zakona o neuspešnih klicih, kjer se podatki pridobivajo ali obdelujejo ali hranijo (pri podatkih o telefoniji) ali beležijo (pri internetnih podatkih) pri izvajalcih javnih komunikacijskih storitev ali operaterjih omrežja. Ta obveznost ne vključuje hrambe podatkov o vsebini komunikacij.

(4) Operaterji lahko hrambo podatkov iz 164. člena tega zakona zagotavljajo tudi skupaj. Agencija lahko operaterju z odločbo naloži, da mora zagotavljati hrambo tudi za druge operaterje, če je to glede na medsebojni poslovni odnos operaterjev primerno in potrebno. Z odločbo odloči tudi o upravičenih stroških operaterja, ki je s tako hrambo obremenjen.

(5) Operaterji zagotavljajo hrambo podatkov iz prvega, tretjega in četrtega odstavka tega člena v skladu z določbami tega zakona za 14 mesecev od dneva komunikacije za podatke v zvezi z javno dostopnimi telefonskimi storitvami ter osem mesecev od dneva komunikacije v zvezi z drugimi podatki.

(6) Pristojni organ, ki odloča o dostopu do podatkov iz prvega odstavka tega člena, lahko na predlog predlagatelja odredbe za dostop do podatkov podaljša rok hrambe za omejen čas, če to upravičujejo posebne okoliščine kazenskega pregona, ki jih določa zakon, ki ureja kazenski postopek, zagotavljanje nacionalne varnosti in ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države, kakor jih določa zakon, ki ureja Slovensko obveščevalno-varnostno agencijo, ter obrambe države, kakor jih določa zakon, ki ureja obrambo države. O tem pristojni organ, ki odloča o dostopu do podatkov, obvesti ministrstvo in informacijskega pooblaščenca. Ministrstvo o podaljšanju hrambe uradno obvesti Evropsko komisijo in druge države članice EU ter navede razloge za podaljšanje. Izvajanje ukrepa se prekine takoj, ko prenehajo posebne okoliščine ali ko pristojni organ, ki je odločil o podaljšanju, prejme obvestilo Evropske komisije o nedopustnosti ukrepa.

(7) Operaterji morajo ob koncu hrambe uničiti vse podatke, ki so jih hranili v skladu z določbami tega poglavja, razen tistih, za katere je bila izdana odredba za dostop in so bili posredovani pristojnemu organu.

164. člen

(vrste podatkov, ki se hranijo)

Podatki, ki se hranijo (v nadaljnjem besedilu: hranjeni podatki), so:

1. podatki, ki so potrebni za odkritje in prepoznanje vira komunikacije in vključujejo:

– pri telefonskih storitvah v fiksnem in mobilnem omrežju telefonsko številko kličočega ter ime in naslov naročnika ali registriranega uporabnika,

– pri dostopu do interneta, elektronske pošte in uporabi telefonije prek internetnega protokola: naslov internetnega protokola, uporabniško ime, telefonsko številko, dodeljeno za vsako komunikacijo, s katero se vstopa v javno telefonsko omrežje, ter ime in naslov naročnika ali registriranega uporabnika, ki mu je bil med komunikacijo dodeljen naslov internetnega protokola, uporabniško ime ali telefonsko številko,

2. podatki, ki so potrebni za prepoznanje cilja komunikacije in vključujejo:

– pri telefonskih storitvah v fiksnem in mobilnem omrežju klicano telefonsko številko in v primerih, ki vključujejo dodatne storitve, kot je preusmeritev ali predaja klica, številko ali številke, na katere je klic preusmerjen, ime in naslov naročnika ali registriranega uporabnika,

– pri dostopu do elektronske pošte in uporabi telefonije prek internetnega protokola: naslov internetnega protokola, uporabniško ime ali telefonsko številko prejemnika klica prek telefonije prek internetnega protokola, ime in naslov naročnika ali registriranega uporabnika in uporabniško ime namembnega prejemnika komunikacije,

3. podatki, ki so potrebni za ugotovitev datuma, časa in trajanja komunikacije ter vključujejo:

– pri telefonskih storitvah v fiksnem in mobilnem omrežju datum ter čas začetka in trajanje ali čas konca komunikacije,

– pri dostopu do interneta datum in čas prijave na internet in odjave z njega, pri čemer se upošteva določen časovni pas, skupaj z naslovom statičnega ali dinamičnega internetnega protokola, ki ga je ponudnik dostopa do interneta dodelil komunikaciji, in uporabniško ime naročnika ali registriranega uporabnika,

– pri uporabi storitev elektronske pošte in telefonije prek internetnega protokola datum in čas pričetka izvajanje storitve ter pri telefoniji prek internetnega protokola tudi čas trajanja ali čas konca izvajanja storitve, pri čemer se upošteva določen časovni pas,

4. podatki, ki so potrebni za ugotovitev vrste komunikacije in vključujejo:

– pri telefonskih storitvah v fiksnem in mobilnem omrežju vrsto uporabljene telefonske storitve,

– pri dostopu do elektronske pošte in uporabi telefonije prek internetnega protokola vrsto uporabljene storitve,

5. podatki, ki so potrebni za razpoznavo komunikacijske opreme uporabnikov in vključujejo:

– pri telefonskih storitvah v fiksnem omrežju kličočo in klicano telefonsko številko,

– pri telefonskih storitvah v mobilnem omrežju kličočo in klicano telefonsko številko, mednarodno identiteto mobilnega naročnika kličoče in klicane stranke, mednarodno identiteto mobilnega terminala kličoče in klicane stranke, pri predplačniških anonimnih storitvah pa datum in čas začetka uporabe storitve ter ID celice, kjer je bila storitev izvedena,

– pri dostopu do interneta, elektronske pošte in uporabi telefonije prek internetnega protokola kličočo telefonsko številko za klicni dostop, digitalni naročniški vod ali drugo končno točko začetnika komunikacije,

6. podatki, ki so potrebni za ugotovitev lokacije opreme za mobilno komunikacijo:

– lokacijska oznaka (ID celice) na začetku komunikacije,

– podatki, ki določajo zemljepisno lego celic z navedbo njihovih lokacijskih oznak med obdobjem, za katero se hranijo podatki o komunikaciji.

165. člen

(zavarovanje hranjenih podatkov)

(1) Operaterji zagotovijo zavarovanje hranjenih podatkov v skladu z zakonom, ki ureja varstvo osebnih podatkov. V zvezi s tem vsak zase ali skupaj sprejmejo primerne tehnične in organizacijske ukrepe, s katerimi hranjene podatke zaščitijo pred uničenjem, izgubo ali spremembo in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkritja.

(2) Operaterji lahko hranjene podatke obdelujejo le v obsegu, ki je nujen za zagotavljanje hrambe.

(3) Hranjeni podatki morajo biti enake kakovosti kakor podatki v omrežju. Za hranjene podatke veljajo določbe tega zakona o varstvu in zaščiti podatkov v omrežju.

(4) Agencija po predhodnem mnenju informacijskega pooblaščenca v splošnem aktu podrobneje predpiše način hranjenja podatkov in način izvajanja tega člena. Agencija izvaja nadzor nad izvajanjem splošnega akta, sprejetega na podlagi te določbe.

166. člen

(posredovanje hranjenih podatkov pristojnim organom)

(1) Operater mora takoj oziroma brez nepotrebnega odlašanja posredovati hranjene podatke od trenutka prejema prepisa tistega dela izreka odredbe pristojnega organa, v katerem je navedba vseh potrebnih podatkov o obsegu dostopa.

(2) Prepis odredbe iz prejšnjega odstavka opravi organ, ki je odredbo izdal.

(3) Operater mora po prejeti odredbi posredovati hranjene podatke pristojnemu organu v obsegu, kakor je določeno v prepisu izreka odredbe.

(4) Operater osebam, ki jih odredba iz prvega ostavka tega člena zadeva, ali tretjim osebam ne sme razkriti te odredbe in da je ali da bo hranjene podatke na podlagi tega člena posredoval pristojnemu organu.

(5) Operaterji morajo skupaj s pristojnimi organi, ki lahko zahtevajo dostop do hranjenih podatkov, zagotoviti desetletno neizbrisno registracijo vsakega sporočanja hranjenih podatkov in v okviru tega roka tudi hraniti pridobljene in izročene podatke od dneva, ko so jih sporočili pristojnemu organu, ter jih varovati v skladu z oznako stopnje tajnosti prepisa odredbe.

(6) Minister v soglasju z ministrom, pristojnim za notranje zadeve, ministrom, pristojnim za obrambo, in direktorjem Slovenske obveščevalno-varnostne agencije podrobneje predpiše način posredovanja hranjenih podatkov.

(7) Informacijski pooblaščenec nadzira izpolnitev obveznosti operaterjev iz tega člena, kar ne posega v pristojnosti nadzora s strani pristojnih organov na podlagi drugih zakonov.

167. člen

(stroški hrambe)

Operaterji morajo na lastne stroške zagotoviti vse potrebne tehnične in organizacijske ukrepe za hrambo podatkov v skladu z določbami tega zakona.

168. člen

(podatki o odredbah o dostopu do podatkov in posredovanja podatkov)

(1) Sodišče, ki je odredilo dostop do podatkov, vodi zbirne podatke o odredbah o dostopu do podatkov in posredovanja podatkov, hranjenih na podlagi 166. člena tega zakona, ki obsegajo:

1. število zadev, v katerih je bil odrejen dostop do hranjenih podatkov,

2. navedbo dneva ali časovnega obdobja, za katero so bili podatki zahtevani, dneva, ko je pristojni organ izdal odredbo o dostopu do podatkov in dneva posredovanja podatkov,

3. število zadev, v katerih odredbe za dostop do podatkov ni bilo mogoče izvršiti.

(2) Pristojno sodišče posreduje zbirne podatke iz prejšnjega odstavka za tekoče leto ministrstvu, pristojnemu za pravosodje, najpozneje do 31. januarja naslednje leto.

(3) Ministrstvo, pristojno za pravosodje, na podlagi prejetih zbirnih podatkov vseh sodišč najpozneje do 20. februarja vsako leto pripravi skupno poročilo o dostopu do hranjenih podatkov za preteklo leto in ga pošlje ministrstvu, ki jih takoj posreduje Evropski komisiji in komisiji državnega zbora, ki je pristojna za nadzor obveščevalnih in varnostnih služb.

(4) Minister, pristojen za pravosodje, po predhodnem mnenju predsednika Vrhovnega sodišča Republike Slovenije, izda navodilo z obrazci za poročanje po tem členu.

169. člen

(nadzor)

Informacijski pooblaščenec ob upoštevanju omejitev iz 166. člena tega zakona nadzira izvajanje določb tega poglavja, razen določb iz četrtega odstavka 165. člena tega zakona, kjer nadzor izvaja agencija.

(II) Razlogi za izpodbijanje določbe ZEKom-1

Kršitev 2. v povezavi z 32., 35., 37., 38. in 39. členom Ustave RS

Ne glede na dejstvo, da izpodbijana zakonska ureditev obvezne hrambe podatkov temelji na Direktivi, Pooblaščenec zatrjujoč, da ureditev krši temeljne človekove pravice in svoboščine posameznikov, zato Ustavnemu sodišču predlaga, da opravi presojo skladnosti obvezne hrambe z URS – po 3.a/I členu URS.

a) Omejitve države pri posegih v posameznikovo zasebno sfero

Pravica do zasebnosti obsega več vidikov; zasebno življenje, družinsko življenje, dom, dopisovanje, informacijsko zasebnost… »Pravica do zasebnosti obstaja pravzaprav v okviru pravice posameznika, da živi svoje življenje z minimalnimi posegi vanj. Zadeva zasebno, družinsko življenje in dom, fizično in moralno integriteto, čast in dobro ime in med drugim tudi razkritje informacij o posamezniku[16]«.

Po 8. členu Evropske konvencije o človekovih pravicah in temeljnih svoboščinah (EKČP) ima vsakdo pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen, če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi.

K vsebini pravice do spoštovanja zasebnega in družinskega življenja iz 8. člena EKČP pa je Evropsko sodišče za človekove pravice dodalo tudi možnost ustvariti in ohraniti vez z drugimi ljudmi za izpolnitev posameznikove osebnosti, ter tudi posameznikovo informacijsko zasebnost.

[16] Council of Europe, Cons.Ass., 21st Ordinary Session, Text Adopted 1970, COE Collected Texts, Strasbourg, 178, citirano po dr. Lampe, Pravo človekovih pravic, Uradni list, Ljubljana 2010.

Glede spoštovanja zasebnosti tako EKČP pred državo postavlja dve zahtevi: 1 – država se ne sme vmešavati v posameznikovo zasebnost; 2 – država mora varovati posameznikovo zasebnost (pred posegi drugih) z nacionalnim pravom[17].

Podobne zahteve pred državo postavlja Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov iz leta 1981 (Konvencija 108).

b) Omejitve države pri posegih v informacijsko in komunikacijsko zasebnost posameznikov

O kršitvah 8. člena EKČP je Evropsko sodišče za človekove pravice (ESČP) sprejelo vrsto odločitev. Za primer obvezne hrambe podatkov o prometu in lokaciji ter z njimi povezanih podatkov, ki določajo naročnika ali uporabnika javne komunikacijske storitve je zanimiva zadeva Klass proti ZRN[18]. Čeprav je ESČP menilo, da 8. člen EKČP v konkretnem primeru ni bil prekršen, je hkrati ugotovilo, da je telefonski pogovor del zasebnega življenja posameznika, obstoj zakona, ki omogoča nadzor nad komunikacijo naključnih posameznikov, pa pomeni grožnjo nadzorstva, ki napada svobodo komuniciranja in posledično poseg javne oblasti v posameznikovo pravico do zasebnosti. Nadalje je ESČP to tezo razvilo v primeru Kruslin proti Franciji[19].

Po 37. členu Ustave RS (URS) je zagotovljena tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Izhajajoč iz zgoraj citiranih določb EKČP in URS je poseg v komunikacijsko zasebnost posameznika dopusten, če:

- je določen z zakonom;
- je nujen v demokratični družbi;
- je namenjen za uvedbo ali potek kazenskega postopka ali za varnost države;
- je odrejen z odločbo sodišča.

Pooblaščenec meni, da že sama obvezna hramba podatkov, ki so povezani s komunikacijo (kdo je klical, koga, kdaj, koliko časa je trajal pogovor… kdo je poslal SMS sporočilo, komu…), zapovedana s strani države pomeni poseg v komunikacijsko zasebnost posameznikov – uporabnikov javnih komunikacijskih storitev. O tem, da so t.i. prometni podatki[20] sestavni del komunikacije in uživajo enako stopnjo varstva kot vsebina sama, se je večkrat izreklo tako ESČP kot Ustavno sodišče[21]. V primeru Copland proti Združenemu kraljestvu[22] je ESČP presodilo, da varstvo zasebnosti velja tako za telefonske komunikacije, kot tudi za elektronsko pošto in uporabo interneta, in da je s stališča varstva zasebnosti nepomembno ali gre za zasebno ali za službeno komunikacijsko sredstvo. Prav tako so presodili, da kršitev predstavlja že samo zbiranje in obdelava prometnih podatkov in s tem potrdili, da so prometni podatki integralni element komunikacij. Kršitev zasebnosti torej ni "le" vpogled v vsebino komunikacij, pač pa tudi vpogled v prometne podatke. Nadalje so v razsodbi zapisali, da je s stališča varstva zasebnosti tudi povsem nepomembno ali so bili podatki "zgolj" zbrani ali pa so bili tudi razkriti tretjim osebam, oziroma uporabljeni proti pritožnici. Tako so se postavili na stališče, da je sporen že sam akt posega, ne pa šele morebitni kasnejši pregled oziroma obdelava prestreženih podatkov in komunikacij s strani tretje osebe. Sledeč opisani argumentaciji Pooblaščenec meni, da je s strani države zapovedana obvezna hramba

[17] Tako tudi dr. Lampe, Pravo človekovih pravic, Uradni list, Ljubljana 2010; pogl. 5.4.2.
[18] Klass in ostali proti Zvezni republiki Nemčiji, no. 28, 6. september 1978.
[19] Kruslin proti Franciji no. 11801/85, 24. april 1990.
[20] Gre za zbirko osebnih podatkov, ki nastane ob uporabi komunikacijskih sredstev in je neločljivo povezana z vsebino komunikacije.
[21] Ustavno sodišče v sodbi Up-106/05 izpostavi, da je v teoriji zastopano stališče, da ni varovana zgolj vsebina komunikacije, temveč tudi okoliščine in dejstva, povezana s komunikacijo. Med te okoliščine in dejstva prav gotovo sodijo podatki o tem, kdo je komuniciral, kdaj in s kom, morda pa tudi druge okoliščine, kot je npr. vrsta uporabljene komunikacije.
[22] Copland proti Združenemu kraljestvu, no. 62617/00, 3. april 2007.

prometnih podatkov po ZEKom-1 poseg v zasebnost uporabnikov javnih komunikacijskih storitev, ki glede na URS ne izpolnjuje vsaj dveh pogojev za njegovo dopustnost; ni nujen v demokratični družbi (glede na obseg hranjenih osebnih podatkov je to po mnenju Pooblaščenca očitno), ni odrejen z določbo sodišča (kar je posledica izjemne nesorazmernosti ukrepa in predvsem dejstva, da za izdajo sodne odredbe za veliko večino hranjenih podatkov sploh ne bi bili izpolnjeni pogoji).

Obvezna hramba podatkov po ZEKom-1 je tako po mnenju Pooblaščenca, ne le z vidika načela pravne države nesorazmeren ukrep, ukrep, ki izničuje v 38. členu URS definirano pravico posameznikov do varstva osebnih podatkov, ampak tudi poseg države v komunikacijsko in informacijsko zasebnost uporabnikov javne komunikacijske storitve, ki je izrecno v nasprotju s 37. členom Ustave RS.

c) Omejitve države pri posegih v svobodo gibanja, pravico do zasebnosti in osebnostnih ter svobodo izražanja

Za demokratične družbe splošno velja, da združujejo svobodne posameznike. Svoboda v pravnem smislu seveda ne pomeni, da lahko posameznik ravna zgolj po svoji volji, ne oziraje se na pravice drugih. Brez dvoma pa pomeni, da mu država ne sme omejevati svobode ravnanja in gibanja, če to ni nujno v demokratični družbi in določeno z zakonom. Med omejitve te svobode ne gre uvrščati zgolj ukrepov, ki posameznika fizično omejujejo v gibanju, mu ga preprečujejo, ampak po mnenju Pooblaščenca tudi ukrepe, ki pomenijo nadzor na ravnanjem posameznika, nad njegovim gibanjem, ne da bi ta isti posameznik s svojimi dejanji državi dal kakršenkoli povod za nadzor. Po sporni ureditvi obvezne hrambe podatkov se hranijo tudi podatki o lokaciji posameznikov – uporabnikov javnih komunikacijskih storitev. Država torej zahteva, da ponudniki komunikacijskih storitev shranijo tudi podatek o tem, od kod (s katere lokacije) je posameznik komuniciral in na ta način nadzirajo gibanje uporabnikov javnih komunikacijskih storitev, ne da bi ti državi dali (vnaprej) kakršenkoli povod za opravičilo kontrole gibanja ob komuniciranju. Ukrep, s katerim država zahteva obvezno hrambo podatkov o lokaciji posameznikov, ki komunicirajo, je po prepričanju Pooblaščenca v očitnem nesorazmerju s koristjo, ki jo lahko država utemeljeno pričakuje od tega ukrepa. Kot smo pojasnili že zgoraj, se podatki obdelujejo zgolj za vsak slučaj – da lahko država (njeni represivni organi) lažje najdejo ali prepoznajo domnevnega storilca kaznivega dejanja, ali tistega, ki domnevno ogroža državno varnost. Tako ni videti razlike v ukrepu obvezne hrambe podatkov in v npr. ukrepu obvezne vsaditve RFID čipa[23] v roke vsake polnoletne osebe. V slednjem primeru bi ponudnik RFID tehnologije za državo shranjeval podatke o lokaciji (gibanju) imetnikov RFID čipov, v primeru kaznivega dejanja (ali drugega nezaželenega ravnanja) pa bi država zgolj preverila, kdo je bil ob kritičnem času na kraju dejanja. Tehnologija na široko odpira vrata utilitarističnemu pristopu k varstvu človekovih pravic, vendar je po prepričanju Pooblaščenca k uporabi tehnologije, ki posega v temelje posameznikove osebnosti, treba pristopati zadržano, preudarno, ob ozki razlagi načela sorazmernosti. Pooblaščenec je prepričan, da so koristi ukrepa minimalne in ne odtehtajo posegov v zasebnost posameznikov. Preprosto povedano, državi ni dopuščeno, da zaradi enostavnosti in (navidezne) zanesljivosti uporabe tehnologij opusti tehtanje o nujnosti posegov in za državo »bolj napornih« alternativah.

Védenje o stalnem nadzoru pri uporabi javnih komunikacijskih kanalov brez dvoma vpliva tudi na izvrševanje svobode izražanja. Posameznik, ki ve, da je nadziran, se bo obnašal drugače – nesvobodno. Bi še napisali kratko sporočilo (SMS ali elektronsko pošto) s kritiko predsednika države, vlade, ministra, če bi vedeli, da bodo podatki, da ste, kdaj ste, s katere lokacije in komu ste poslali sporočilo še 14 mesecev shranjeni za državo – za

[23] Radiofrekvenčna identifikacija (angleško Radio Frequency IDentification, kratica **RFID**) je tehnologija za prenos podatkov med čitalcem in elektronsko oznako v namen identifikacije. Oznaka je sestavljena iz integriranega vezja (čipa), ki hrani in procesira podatke, ter izvaja modulacijo in demodulacijo signalov. Drugi del oddajnika je antena, ki sprejema in oddaja radijske signale. Signale RFID oddajnikov sprejema RFID čitalec, kar omogoča identifikacijo predmetov oziroma bitij, na katere je oddajnik pritrjen. RFID identifikacijska tehnologija naj bi postopoma izpodrinila črtne kode

isto države, katere visoke uradnike ste kritizirali,?! Bi to še storili, čeprav ni kaznivo in obstaja zato velika stopnja verjetnosti, da sporočila državni organi v resnici ne bodo prebrali? Pooblaščenec je prepričan, da védenje o nadzoru komunikacij z obvezno hrambo podatkov vpliva na samocenzuro posameznika in zmanjšuje dejansko svobodo izražanja. Pravica do zasebnosti in pravica do varstva osebnih podatkov je v kontekstu prej navedenega lahko razumljena tudi kot pravica, ki pomaga izvrševati pravico do svobode izražanja iz 39. člena Ustave RS.

d) Korist, ki naj bi jo država pričakovala od obvezne hrambe

Razlog za regulacijo obvezne hrambe podatkov o prometu in lokaciji uporabnikov javnih komunikacijskih storitev naj bi bila boljša raziskanost (hujših) kaznivih dejanj. Zelo pomembnemu delu zasebnosti naj bi se torej odrekli zaradi večje javne varnosti. Seveda pa test sorazmernosti terja več kot le obljubo večje javne varnosti – terja dejanske učinke te obljube v realnosti.

Pooblaščenec želi v uvodu razprave o učinkih – koristih ukrepa obvezne hrambe opozoriti na prevladujoče in povsem zmotno prepričanje o vrednosti avtomatsko generiranih podatkov, med katere sodijo tudi podatki o prometu in lokaciji uporabnikov javne komunikacijske storitve. Računalniško generirane podatke običajno dojemamo kot zaupanja vredne same po sebi in praviloma ne pomislimo na možnost, da so podatki spremenjeni oziroma ponarejeni. Gre za t.i. inherentno zaupanje[24]. Ker torej na predpostavki o pravilnosti in točnosti takšnih podatkov slonijo nadaljnje predpostavke o identiteti klicatelja, ima spreminjanje klicne identifikacije lahko resne posledice. V ZDA se je po letu 2002 pojavilo večje število zlorab, poimenovanih *swatting*. V teh primerih napadalci s ponarejeno klicno identifikacijo kličejo na številko za klic v sili oziroma policijo in trdijo, da zadržujejo talce. Policija se odzove s prihodom specialne enote (t.i. SWAT - Special Weapons and Tactics), kar seveda povzroči obilo nevšečnosti pravim lastnikom telefonske številke. Tehnični ukrepi proti spreminjanju klicne identifikacije niso mogoči. Drug primer zlorabe je takšen, da napadalci najprej pridobijo dostop do bančnega računa žrtve, nato pa med tem, ko izvajajo bančne transakcije, žrtev zasujejo s klici iz naključno ustvarjenih telefonskih številk. S tem preprečijo, da bi banka, ki zazna sumljive transakcije, uspela priklicati svojo stranko in preveriti sumljivost transakcij. Ker so telefonske številke naključno ustvarjene, jih žrtev tudi ne more blokirati. Znan je tudi primer z začetka leta 2012, ko so neznani napadalci v Veliki Britaniji s pomočjo spremenjene klicne identifikacije izvajali masovno klicanje posameznikov (tudi do 1000 klicev na uro). Napadalci so uporabljali klicne identifikacije obstoječih podjetij ter klicne identifikacije neobstoječih številk (kar je številne klicane osebe prestrašilo), zvezo pa so vzpostavili le do točke, da je klicana številka pozvonila, nato pa prekinili. Domnevno naj bi bil razlog tega početja v preverjanju, katere telefonske številke sploh obstajajo, te podatke pa bi napadalci naprej prodali marketinškim podjetjem za potrebe nelegalnega oglaševanja[25].

Takšne (ponarejene) klice je teoretično sicer mogoče izslediti, v praksi pa je to zelo težko, saj se napadalec z nekaj triki lahko dobro prikrije. Zlonamerni klic je treba najprej izslediti do izvornega operaterja, ki je napadalcu omogočil medoperaterski dostop, nato pa še preko interneta do dejanskega napadalca. Pri tem je treba vedeti, da posredovanje klicev med operaterji lahko poteka na dva načina. V prvem primeru, npr. neki manjši operater A pri večjem ponudniku telefonije B zakupi določen nabor telefonskih številk, posredovanje klicev pa nato poteka preko tega večjega operaterja. V primeru klica od operaterja A preko B do končnega operaterja C, bi končni operater C videl, da je klic prišel od operaterja B. Preiskovalci bi nato morali iti do operaterja B in pri njem pridobiti podatke o tem, od kje so prišli klici iz njegovega omrežja. Vendar pa ni nujno, da operater B hrani

[24] Tako Matej Kovačič v članku: Zaupanje digitalnim dokazom in prometnim podatkom v mobilni tehnologiji (http://hr-cjpc.si/pravokator/wp-content/uploads/2012/11/Zaupanje_digitalnim_dokazom_in_prometnim_podatkom_v_mobilni_telefoniji_Kovacic2012.pdf).
[25] Vsi primeri so iz že omenjenega članka M Kovačiča.

prometne podatke o klicih, ki jih posreduje, saj za te klice hramba prometnih podatkov ni obvezna. Druga možnost je, da ponudnik telefonije sklene neposredno pogodbo z mednarodnimi ponudniki (tim. *agregatorji*). V tem primeru končni operater vidi le, da je klic prišel iz tujine, ne pa tudi, od katerega konkretnega operaterja. Podatke za sledenje je torej potrebno iskati pri agregatorju. Poleg tega gredo pri kakšnih "sivih" ponudnikih telefonije povezave pogosto preko različnih posredniških operaterjev, zato je sledenje izvora takega klica zelo težavno, če že ne povsem nemogoče. Ponudniki na mednarodnem trgu namreč ponujajo povezave različnih kvalitet. Povezave, ki so zelo poceni, so navadno preusmerjene preko različnih držav in različnih ponudnikov, to pa preiskovalcem še dodatno oteži izsledite v izvora klica[26].

Klicno identifikacijo je torej mogoče (relativno enostavno) ponarediti. V tem primeru se pri operaterju - v okviru obvezne hrambe podatkov - dejansko zabeleži ponarejena in ne prava klicna identifikacija. Možnost vpliva na podatke, ki se obvezno hranijo, seveda bistveno relativizira njihovo dokazno vrednost. Izkaže se namreč, da podatki niso vredni zaupanja sami po sebi, ampak bi jih morali razumeti zgolj kot indic – informacijo, ki je izhodišče za ugotavljanje dejanskega stanja (ne pa dejansko stanje samo).

Če zgornje poudarke povežemo s pričakovanimi koristmi države od obvezne hrambe podatkov, lahko zaključimo, da država kot kaže pričakuje, da bodo (hujša) kazniva dejanja izvrševali nevedni in nespretni storilci, ki bodo naivno mislili, da jih represivni organi ne bodo prepoznali kot naročnikov telefonskih številk. Ker je takšno pričakovanje povsem neutemeljeno v realnem življenju, saj so storilci kaznivih dejanj od enostavnega varovala, ki so ga zanje predstavljali predplačniški telefoni, prešli na ponarejanje klicne identitete, lahko na koncu ugotovimo, da bodo slej ali prej v zbirki podatkov, ki se obvezno hranijo, zgolj in samo nedolžni sleherniki. Storilcev (hujših) kaznivih dejanj v tej zbirki ne bo mogoče najti. Nekdo, ki tihotapi prepovedane droge, belo blago ipd., bo našel tako finančna sredstva kot tudi čas, da zabriše (pokvari) svoje sledi v elektronskem svetu.

Korist, ki jo država pričakuje od obvezne hrambe podatkov, bo slej ali prej enaka nič, oziroma se bo prevesila na drugo stran – v škodo, ki jo bodo zaradi neupravičenega zaupanja avtomatično generiranim podatkom, utrpeli resnično nedolžni posamezniki, ki bodo povlečeni v preiskave kaznivih dejanj, ker bo na njihovo udeležbo kazala ponarejena klicna identiteta. Ob predpostavki, da so operaterji stroške obvezne hrambe podatkov prevalili na končne uporabnike, se lahko upravičeno vprašamo, zakaj moramo sami plačevati hrambo podatkov o nas samih, država pa ne zna dokazati, da je to sploh nujno, učinkovito in sorazmerno s posegom v naše pravice[27]?

e) Nesorazmerna prizadetost ustavnih pravic posameznikov zaradi obvezne hrambe podatkov

Ustavno sodišče je v svoji praksi že večkrat odločilo, da je poseg v ustavne pravice dopusten, če je v skladu s t.i. načelom sorazmernosti nujen, primeren in sorazmeren v ožjem smislu:
1. poseg mora biti nujen - v tem smislu, da cilja ni mogoče doseči z nobenim blažjim posegom v ustavno pravico ali celo brez njega;
2. poseg mora biti primeren za dosego zaželenega, ustavno dopustnega cilja - primeren v tistem smislu, da je z njim ta cilj možno doseči, in
3. poseg mora biti sorazmeren v ožjem smislu, kar pomeni, da je pri ocenjevanju nujnosti posega treba tudi tehtati pomembnost s posegom prizadete pravice v primerjavi s pravico, ki se s tem posegom želi zavarovati, in odmeriti nujnost posega sorazmerno s težo prizadetih posledic[28].

[26] Vse povzeto po članku M. Kovačiča (stran 13).
[27] Glej Jure Logar, Občutljivo vprašanje uvajanja novih policijskih pooblastil, Pravna praksa št. 5, 2013, GV Založba, Ljubljana.

[28] Tako že v odločbi Ustavnega sodišča št. U-I-137/93 z dne 2. 6. 1994.

Ad1) Obvezna hramba podatkov po prepričanju Pooblaščenca ni nujna za boljšo raziskanost (hujših) kaznivih dejanj, varnost in obrambo države. Vsi ti cilji so se pred uvedbo obvezne hrambe, glede na dostopne podatke nič slabše kot potem, dosegali na druge načine.

Ad2) Glede na pretirano in apriorno zaupanje digitalnim dokazom ter relativno enostavne možnosti ponarejanja klicne identifikacije po prepričanju Pooblaščenca ta ukrep sploh ni primeren za doseganje cilja – boljše raziskanosti (hujših) kaznivih dejanj, varnost in obrambo države.

Ad3) Po podatkih SURS je bilo v letu 2011 poslanih in posledično obvezno shranjenih 1,5 milijarde podatkov o poslanih kratkih – SMS sporočil, 2 milijardi odhodnih klicev v mobilni telefoniji, 500 milijonih klicev v fiksni telefoniji, 32 milijonih MMS sporočil, podatkov o prometu na internetu in e-pošti niso izmerili[29]. Glede na dejstvo, da je zavezanec (Si.mobil d.d.) v letih 2007 – 2012 prejel 373, 688, 692 oziroma 583 zahtev[30] za posredovanje podatkov, ki se hranijo, zahteve pa se pošiljajo vsem operaterjem, saj policija (tožilstvo) praviloma ne ve, kateri operater je shranil podatke, ki jih išče, je očitno, da država povprašuje letno po manj kot 0,012% shranjenih osebnih podatkih. Kako v postopku ti podatki vplivajo na raziskanost kaznivega dejanja, ali so zato postopki končani hitreje in pripeljejo do obsodilnih sodb, zaradi katerih je pričakovanje javnosti po večji javni varnosti utemeljeno, kot smo že zapisali zgoraj, Pooblaščenec zaradi popolnega pomanjkanja tovrstne statistike ni mogel ugotoviti. Ne glede na to smo prepričani, da podatki govorijo sami zase, in da ob tem ne more biti dvoma, da obvezna hramba podatkov glede na korist, ki jo prinaša javni varnosti, očitno prekomerno posega v pravice posameznikov do svobode gibanja, izražanja, tajnost komunikacij, varstva zasebnosti in varstva osebnih podatkov.

V inšpekcijskem postopku je bil zaznan problem širitve prvotnega namena obdelave (ang. t.i. function creep). Podatki iz retencijske zbirke prometnih podatkov so se zahtevali tudi za potrebe pravdnih, prekrškovnih in delovno-pravnih sporov. Ne samo da zakonodajalec ni omejil zbiranja obravnavanih osebnih podatkov za namen obravnavanja hudih kaznivih dejanj, organi so pričeli podatke zahtevati tudi za namene, ki so povsem izven tistega, zaradi katerega se podatki sploh zbirajo.

Kršitev 3.a/III člena Ustave RS

Če bi Ustavno sodišče ocenilo, da je obvezna hramba podatkov o prometu v javnem komunikacijskem omrežju skladna z ustavnimi pravicami posameznikov po URS (upoštevaje 3.a/I člen URS), Pooblaščenec predlaga, da opravi še presojo o tem, ali je bila pri prenosu ureditve obvezne hrambe iz Direktive v ZEKom-1 spoštovana pravna ureditev EU ali ne - po 3.a/III členu URS.

Po tretjem odstavku 3.a člena Ustave RS se pravni akti in odločitve, sprejeti v okviru mednarodnih organizacij, na katere Slovenija prenese izvrševanje dela suverenih pravic, v Sloveniji uporabljajo v skladu s pravno ureditvijo teh organizacij. Uporaba pravnih aktov in odločitev v skladu s pravno ureditvijo mednarodnih organizacij je tesno povezana s prenosom izvrševanja dela suverenih pravic. Uporabo virov prava EU je tako treba razumeti v najširšem pomenu, tako glede vprašanja, kako to pravo vstopa v slovenski pravni red, kot tudi glede vprašanja, kako v njem učinkuje. Sekundarno pravo EU je samostojno (avtonomno) v tem smislu, da je izraz originarne zakonodajne pristojnosti EU, ki za svojo veljavnost v notranjem pravnem redu držav članic ne potrebuje naknadne odobritve zakonodajnih ali izvršilnih organov držav članic[31].

Sekundarno pravo lahko opredelimo kot skupek vseh normativnih aktov, ki so jih EU institucije sprejele na osnovi pogodbenih določb. V sekundarno pravo sodijo zavezujoči (uredbe, direktive in sklepi) in nezavezujoči

[29] Vir SURS: http://www.stat.si/novica_prikazi.aspx?id=4965
[30] Glej zapisnik št. 0613-18/2013/1 z dne 23.1.2013.
[31] Tako tudi v Komentarju Ustave RS – dopolnitev A; Evropska fakulteta za državne in evropske študije; Ljubljana, 2011.

pravni akti (priporočila, mnenja), predvideni v Lizbonski pogodbi, ter tudi cela vrsta drugih aktov, kot so poslovniki institucij, akcijski programi Evropske unije, itd. Primarnost prava EU sicer ni navedena v izrecni določbi Pogodbe, temveč je razvidna iz sodne prakse Sodišča EU. Primarnost prava EU zagotavlja, da nacionalno pravo ne more razveljaviti prava EU niti ga ne more spreminjati in da ima to v primeru neskladja prednost pred nacionalnim pravom.

Direktiva v 1/I. členu določa:
Namen te direktive je uskladiti določbe držav članic glede obveznosti ponudnikov javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij glede hrambe določenih podatkov, ki jih pridobivajo ali obdelujejo, da se zagotovi dostopnost podatkov za namen preprečevanja, preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic

Direktiva je bila v ZEKom-1 prenesena tako, da je bistveno razširila »uporabnost« (namen) obvezno shranjenih osebnih podatkov uporabnikov javnega komunikacijskega omrežja. Tako se ti podatki po ZEKom-1 lahko uporabijo:

- za namene, 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 namene obrambe države, kakor jih določa zakon, ki ureja obrambo države.

Kot vsaka direktiva je tudi Direktiva namenjena usklajevanju pravnih ureditev držav članic - tokrat na področju obvezne hrambe podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij. Cilj takšne usklajenosti pa je zagotavljanje enakih pravic in obveznosti vsem pravnim in fizičnim osebam na območju Evropske unije. Direktiva mora biti kot sekundarni pravni vir prenesena neposredno in popolnoma. V primeru prenosa Direktive ni bilo tako, zato so izpodbijane določbe ZEKom-1 (tudi) v nasprotju s 3.a/III členom URS.

Izpodbijane določbe ZEKom-1 so po oceni vlagatelja zahteve v neskladju z 2. v povezavi z 32., 35., 37., 38. in 39. členom Ustave RS oziroma v neskladju s 3.a/III členom Ustave RS, zato Pooblaščenec

p r e d l a g a:

da Ustavno sodišče RS na podlagi 4. alineje 1. odstavka 21. člena ZUstS oceni ustavnost izpodbijanih določb, ugotovi njihovo neskladnost z Ustavo ter jih na podlagi 1. odstavka 45. člena ZUstS razveljavi.

Informacijski pooblaščenec:
Nataša Pirc Musar, univ. dipl. prav.,
pooblaščenka