

Zasebnost in hramba prometnih podatkov v mobilni telefoniji

Matej Kovačič¹¹

POVZETEK: Besedilo se ukvarja z vprašanjem informacijske zasebnosti na področju mobilnih komunikacij, konkretnije z vprašanjem beleženja in hrambe prometnih podatkov v mobilni telefoniji. Evropska unija je namreč za razliko od ZDA v preteklosti z Direktivo o zasebnosti in elektronskih komunikacijah²²

hrambo prometnih podatkov načeloma prepovedovala, s sprejemom Direktive o obvezni hrambi prometnih podatkov³³ pa se je to načelo povsem spremenilo in hramba prometnih podatkov je od konca leta 2006 uzakonjena tudi v Sloveniji. Del besedila je posvečen tudi hrambi prometnih podatkov v Sloveniji ter njihovi uporabi v kazenskem postopku.

1.0 Uvod

Leta 1791 je angleški pravnik in filozof Jeremy Bentham predstavil načrt zapora Panoptikon. Zapor sicer ni bil nikoli zgrajen, kljub temu pa je bila Benthamova ideja na nek način revolucionarna, saj je oblikovala idejo nadzora kot tehnologije oblasti. V središče Panoptikona je Bentham postavil nevidnega nadzornika, ki ima v vsakem trenutku pregled nad zaporniki. Osnovna ideja Panoptikona je asimetrični nadzor, Benthamov izum pa je pravzaprav tehnologija oblasti. Foucault pravi, da ta asimetričen nadzor služi funkcioniranju oblasti na mikroravni: »Kdor je podrejen polju vidnosti in to ve, sam prevzame prisile oblasti; spontano jih uporablja na samem sebi; vase vtisne oblastno razmerje, v katerem igra hkrati obe vlogi: postane načelo svoje lastne podvrženosti« (Foucault 1984: 202). Še več: obvladovanje posameznikov v Panoptikonu gre tako daleč, da se skuša posameznika ne samo prisiliti, da se obnaša tako, kot je to od njega zahtevano, pač pa da se mu celo želi odvzeti svobodno voljo, da ne bi sploh pomislil, da bi kaj storil narobe. Foucault pravi: »Bentham je v svojem tekstu zelo jasno zapisal, kako pomembno je odvrčanje. 'Zelo važno je', pravi, 'da ima Inšpektor zapornika neprestano na očeh; tako mu skorajda ne bo prišlo na misel, da bi storil kaj narobe.' S tem smo se znašli v srcu revolucionarnih prizadevanj: kako preprečiti ljudem, da bi storili kaj narobe, kako izničiti njihovo željo, da bi grešili. Skratka, kako jim odvzeti zmožnost in voljo.« (Foucault 1991: 47). To oblast, katere

¹ Dr. Matej Kovačič (matej.kovacic@fdv.uni-lj.si) je asistent na Fakulteti za družbene vede, Univerza v Ljubljani.

² Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

³ Direktiva 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 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

značilnost je, da se izvaja konstantno in s pomočjo nadzorovanja (Foucault 1991: 37), Foucault poimenuje disciplinarna oblast.

Foucault pa je ugotovil, da je po 18. stoletju začelo prihajati še do enega premika. Disciplinski oblasti, ki je usmerjena k nadzorovanju posameznika, se je pridružila še oblast, ki je usmerjena k nadzorovanju populacije. Pojavi se statistično spremljanje pojavov, iskanje globalnih kazalcev in povprečnih vrednosti ter uvedbo regulacijskih mehanizmov na tej globalni ravni. Njihov namen je ohranjanje globalnega ravnotežja, povprečja, pravzaprav namestitve varnostnih mehanizmov okrog naključnosti, ki se ji reče življenje (Foucault 1997/2003: 156).

To oblast Foucault poimenuje regulacijska, namenjena pa je pridobivanju védenja zaradi upravljanja (kontrole). Whitaker pravi, da je 20. stoletje stoletje obveščevalne dejavnosti, pri čemer je zanj obveščevalna dejavnost »avtomatsko in namensko pridobivanje, sortiranje, nadomeščanje, analiza, interpretacija in zaščita informacij. ... sistematično organizirana birokratska aktivnost ... s svojo pol-avtonomno vlogo v globalni politiki« (Whitaker 1999: 5). Ta nova regulacijska tehnologija oblasti, ki ravno tako temelji na nadzorovanju, pa ne zamenja prejšnje disciplinske tehnologije, pač pa z njo deluje vzporedno. Foucault pravi, da nova regulacijska oblast disciplinsko: »zaobseže, integrira, deloma spremeni, predvsem pa jo izkorišča za to, da se vanjo na nek način vsadi, ter se s pomočjo te predhodne disciplinarne tehnike dejansko utrdi. ... Povedano drugače: disciplina poskuša vladati množici ljudi, kolikor more in mora ta množica razpasti na individualna telesa, ki jih je mogoče nadzorovati, dresirati, izkoriščati ter morebiti kaznovati.

Nova tehnologija pa se naslavlja na množico ljudi, toda ne kolikor so ti ljudje zvedeni na telesa, temveč nasprotno, kolikor ta tehnologija oblikuje neko globalno množico, ki jo zadevajo skupni procesi ...« (Foucault 1997/2003: 153–154). S tem pa ta nova tehnologija oblasti prejšnjo celo nadgradi. Foucault govori o normalizacijski družbi, kjer se sekata disciplina in regulacija (Foucault 1997/2003: 161). Ključna tehnologija oblasti v družbah discipline in regulacije je nadzor, s čimer vstopamo v družbe nadzora, »ki ne funkcionirajo s pomočjo zapiranja, pač pa s pomočjo nenehnega nadzora in hipne komunikacije« (Deleuze 2002: 171). Zanje je značilen nadzor, ki je »kratkega roka in hitrega kroženja, toda tudi nenehen in brezmejen«, ugotavlja Deleuze (Deleuze 2002: 176).

Ključna nadzorna tehnologija je dandanes informacijska tehnologija. Če je Benthamov načrt Panoptikona predvideval optični nadzor, pa v informacijski družbi vidnost ni več samo optična, pač pa se večina današnjega nadzora pojavlja na območju digitalnih signalov in prometnih podatkov, ki se zbirajo in shranjujejo samodejno in vsaj nekaj časa tudi hranijo. Zato so danes baze podatkov eno glavnih orodij množičnega nadzora.

Sodobna informacijsko-komunikacijska tehnologija pa ne omogoča samo zbiranja velikega števila podatkov, pač pa tudi njegovo povezovanje. Nadzor zato lahko postane razpršen, tehnologija pa omogoča povezavo in obdelavo razpršenih podatkov. Nove razsežnosti nadzora vzpostavljajo tudi napredne statistične tehnike, kot na primer tehnike izkopavanja podatkov (ang. data mining) ter sistemi umetne inteligence. S tem se dogaja preskok na novo raven, na raven preventive in predvidevanja.

Sodobna panoptična tehnologija tako ne čaka, da se nekaj zgodi, pač pa ukrepa že vnaprej na podlagi zbranih podatkov in ocenjenih predvidevanj. Množični podatkovni nadzor danes postaja rutinski in je čedalje bolj namenjen profiliranju posameznikov (njihovemu razvrščanju v kategorije).

Čedalje bolj pomembne usmeritve v razvoju sodobnih nadzorovalnih sistemov postajajo preventiva, predvidevanje in katalogiziranje.

Poleg tega je podatkovni nadzor načeloma neviden, posameznik pa pogosto niti

nima možnosti, da bi se mu izognil. Varnost in udobje sta postala glavna argumenta, za katerima je mogoče vedno znova skriti nove oblike nadzora. Zato nadzorovanje postaja čedalje bolj obsežno, nezaznavno, instrumentalizirano, neselektivno in preventivno. Z množično rabo nadzor spodkopava človekove pravice in svoboščine, saj možnosti zlorabe ne ležijo zgolj v neupravičeni oz. nepooblašteni uporabi tehnologij nadzora, pač pa tudi v njeni prepogosti rabi s strani tistih, ki so jih sicer upravičeni uporabljati (Šelih 1979: 157)

2.0 Informacijska in komunikacijska zasebnost ter prometni podatki

Pravica do zasebnosti je navadno določena kot »meja, do katere družba lahko vdre v posameznikove zadeve« (Laurant 2003: 1), čeprav je problem definicije veliko bolj večplasten, saj je, kot ugotavljajo številni avtorji (Wagner DeCew, Agre, Sykes, Bennett in drugi), zasebnost zelo slabo definirana, dodaten problem pa predstavljajo še kolizije drugih pravic z zasebnostjo. Niti v mednarodnem niti v slovenskem pravu zasebnost ni natančno definirana. Celo nasprotno: Evropsko sodišče za človekove pravice je v primeru Niemietz proti Nemčiji leta 1992 poudarilo, da natančne definicije pojma zasebnosti ni mogoče podati (to pa seveda ne pomeni, da se sme zasebnost razlagati restriktivno): »Sodišče ne smatra, da je mogoče ali nujno poizkusiti podati izčrpno definicijo 'zasebnega življenja'«. ⁴

Zasebnost prihaja v kolizijo tudi z različnimi interesi, zato včasih ne more biti varovana zaradi pravnih in družbenih razlogov (Wagner DeCew 1997: 28), poleg tega je dojemanje zasebnosti s strani posameznika relativno in odvisno od konteksta (Wagner DeCew 1997: 29 ter Cate v Etzioni 1999: 199).

Zasebnost posamezniku omogoča, da se umakne izpred oči drugih, a z omejitvijo dostopa ne izolira ljudi, pač pa jim omogoča, da se z drugimi združujejo na avtonomen način, s čimer se povečuje zmožnost ustvarjanja novih in globljih odnosov. Zasebnost torej povečuje zmožnost posameznika, da avtonomno in neodvisno od okolice vzpostavlja odnose z drugimi. DeCewova pravi, da zasebnost omogoča samostojno izbiro osebnih dejavnosti posameznika ter samostojno odločitev, kakšne odnose bo vzpostavljala brez vmešavanja drugih (Wagner DeCew 1997: 66, 69). Podobnega mnenja je tudi Šelihova, ki pravi, da zasebnost posamezniku omogoča, da najde samega sebe, s čimer postaja avtonomen, to pa mu omogoča, da »konstruktivno sodeluje z drugimi in se vključuje v družbo« (Šelih 1979: 176). Ne gre torej samo za vrednoto posameznika, pač pa za vrednoto, ki je pomembna za celotno družbo. Po mnenju Šelihove se pri pravici do zasebnosti »splošni interes kaže prav prek posameznikovega interesa« (Šelih 1979: 31). Zato nekateri zasebnosti ne vidijo kot samo osebnostne pravice, pač pa kot neke vrste družbeno pravico (Šelih 1979: 151).

Zasebnost delimo na več dimenzij, ki pa so med seboj prepletene. Različni avtorji navajajo različne dimenzije zasebnosti, med bolj uveljavljenimi pa je klasifikacija avtorjev poročila Privacy & Human Rights, ki zasebnost deli na informacijsko, komunikacijsko, prostorsko ter zasebnost telesa. Informacijska zasebnost se navezuje na obdelavo osebnih podatkov in je znana tudi kot zaščita (osebnih) podatkov. Gre za možnost posameznika, da obdrži podatke in informacije o sebi, ker si ne želi, da bi bili z njimi seznanjeni drugi (Čebulj 1992: 7). Komunikacijska zasebnost pa ščiti posameznikove komunikacije pred prestrežanjem s strani

⁴ Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

drugih. Nekateri avtorji informacijske zasebnosti ne ločujejo od komunikacijske (Wagner DeCew 1997: 75–78, pa tudi Lampe 2004: 49), v splošnem pa seveda velja, da sta obe dimenziji tesno prepleteni.

2. 1 Informacijska zasebnost

Kot rečeno, informacijska zasebnost se nanaša na osebne podatke, ki se zbirajo v različnih bazah podatkov. Mednje lahko štejemo tudi prometne podatke, ki nastajajo ob uporabi komunikacijskih sredstev (npr. mobilnega telefona, interneta itd.). Informacijska zasebnost se je kot posebna dimenzija izraziteje pojavila v 60. in 70. letih 20. stoletja, vendar je bila v tem času razumljena predvsem kot problem, ki je obstajal večinoma znotraj nacionalnih držav. V 80. letih in kasneje pa je zaradi razvoja in povečane dostopnosti tehnologije informacijska zasebnost postala izrazito mednarodni izziv (Bennett 2001: 103). Zato je Organizacija za ekonomsko sodelovanje in razvoj 23. septembra 1980 sprejela Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), leto dni kasneje pa je Svet Evrope sprejel Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.⁵⁵

Informacijsko zasebnost je kasneje (leta 1995) zaščitila še EU z Direktivo o varstvu osebnih podatkov 95/46/EC.⁶⁶

To kaže, da je informacijska zasebnost pomembno področje, ki je regulirano tudi z mednarodnim pravom. Kljub vsemu velja omeniti, da je za razliko od Evrope v ZDA informacijska zasebnost zunaj doma in konteksta vladnega preiskovanja in zaplembe slabo varovana (Cate 1997: 65), pravna ureditev teh področij pa je nesistematična in včasih že kar dvolična. Delno to velja tudi za komunikacijsko zasebnost. Načeloma namreč v ZDA na zvezni ravni za zasebni sektor ne veljajo skoraj nikakršne omejitve pri zbiranju in obdelavi osebnih podatkov. Nekatere zvezne države imajo sicer urejene nekatere vidike varstva zasebnosti tudi na področju zasebnega sektorja (Laurant 2003: 529), vendar pa ameriški pravni sistem že v samem temelju otežuje izenačitev varstva informacijske zasebnosti v javnem in zasebnem sektorju, saj bi bila lahko previsoka stopnja zaščite informacijske zasebnosti v zasebnem sektorju na ravni posamezne zvezne države v nasprotju s prvim amandmajem ameriške ustave,⁷

ki zagotavlja svobodo govora, na kar kaže primer US West proti FCC,⁸⁸ kjer je zvezno Prizivno sodišče desetega okrožja presodilo, da so osebni podatki, ki jih zbere podjetje, »vrsta govora« in je zato uporaba potrošnikovih podatkov s strani tretje stranke v poslovnih transakcijah poslovni govor, ki je zaščiten s prvim amandmajem« (White 2003: 24).

2. 2 Komunikacijska zasebnost

Komunikacijska zasebnost je ena bolj znanih dimenzij zasebnosti. V Evropi⁸.

⁵⁵ Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je Državni zbor Republike Slovenije ratificiral dne 25. 1. 1994. Veljati je začela dne 1. 3. 1994.

⁶⁶ Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 – 0050.

⁷ 1. amandma, Listina svoboščin (Bill of Rights), 1791.

⁸ U.S. West v. F.C.C., 182 F.3d 1224 (1999).

člen Evropske konvencije o človekovih pravicah⁹ vsakomur priznava tajnost pisem in drugih občil.¹⁰

Občila oz. komunikacijska sredstva se v tem primeru razlagajo zelo široko, torej kot telefonske komunikacije, elektronska pošta, SMS -sporočila itd., saj oblika in vsebina sporazumevanja ni pomembna.

Pravica do komunikacijske zasebnosti je razmeroma dobro zavarovana, seveda pa ni absolutna. Evropsko sodišče za človekove pravice je tako v primeru Klaas in drugi proti Nemčiji¹¹ leta 1978 zapisalo, da je tajen nadzor telekomunikacij nujno potreben element zagotavljanja nacionalne varnosti (Klemenčič 2002: 398). Za tak ukrep je potrebna sodna odredba oziroma ustrezna zakonska podlaga, vendar je slednja v nekaterih primerih lahko razmeroma široka. V Nemčiji npr. tajna služba BND (Bundesnachrichtendienst) po razsodbi ustavnega sodišča iz leta 1999 sme prisluškovati mednarodnim komunikacijam avtomatsko in brez sodnega naloga (t. i. screening metoda)¹² v primerih preprečevanja terorizma in nelegalne trgovine z orožjem in drogami (Laurant 2003: 249). Po drugi strani pa je komunikacijska zasebnost v evropski pravni praksi definirana dovolj široko in pokriva tako zasebna kot službena in druga komunikacijska sredstva. Evropsko sodišče za človekove pravice je leta 1998 v primeru Lambert proti Franciji¹³ jasno poudarilo, da glede tajnosti komunikacij ni razlike med lastnim telefonskim priključkom ali telefonskim priključkom tretje osebe; istega leta pa v primeru Kopp proti Švici¹⁴, da so zaščiteni tudi klici iz poslovnih prostorov ter v poslovne prostore. Prav tako so pred posegi delodajalca zaščiteni tudi komunikacijska sredstva, ki jih na delovnem mestu uporablja zaposleni (npr. odločitev Halford proti Veliki Britaniji¹⁵ iz leta 1997 ter odločitev Kasacijskega sodišča Francije v primeru Societe Nikon France, SA v. Onof, št. 99–42.942 iz leta 2001).¹⁶

⁹ Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, Mednarodne pogodbe, št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

¹⁰ 8. člen Evropske konvencije o varstvu človekovih pravic in mednarodnih svoboščin (Pravica do spoštovanja zasebnega in družinskega življenja) pravi: »1. Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. 2. 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 zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.«

¹¹ Klaas et. al v. ZR Nemčija, odločba z dne 6. 9. 1978.

¹² Vendar pa morajo biti iskalni pojmi, ki jih uporabljajo avtomatski iskalniki, odobreni s strani t. i. G10 komiteja (Temporary Committee on the ECHELON Interception System, 2001: 23).

¹³ Lambert v. Francija, odločba z dne 24. 8. 1998.

¹⁴ Kopp v. Švica, odločba z dne 25. 3. 1998.

¹⁵ Halford v. Velika Britanija, odločba z dne 25. 6. 1997.

¹⁶ V primeru Halford proti Veliki Britaniji je policija nadzorovala službeni telefon svoje uslužbenke z namenom, da bi zbrala gradivo za svojo obrambo v postopku zaradi diskriminacije, ESČP pa je v razsodbi izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost. Podobno stališče v zvezi z uporabo interneta in elektronske pošte na delovnem mestu je v začetku leta 2007 zavzelo ESČP tudi v sodbi Copland proti Veliki Britaniji. Odločitev Kasacijskega sodišča Francije št. 99–42.942 iz leta 2001 pa izrecno pravi, da »delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci

2.3 Zasebnost na področju telekomunikacij

Če za zasebnost vsebine komunikacij velja, da je razmeroma natančno opredeljena in da glede njenega varstva obstajajo razmeroma enotni standardi, pa se v zadnjih letih največ sprememb dogaja na področju zasebnosti t. i. prometnih podatkov.

Enotni standardi varstva zasebnosti na področju telekomunikacij in elektronskih komunikacij v Evropi so bili sicer postavljeni že z Evropsko konvencijo o človekovih pravicah,¹⁷ še nekoliko bolj pa sta jih konkretizirali dve direktivi EU. Leta 1997 je bila sprejeta Direktiva o zasebnosti telekomunikacij 97/66/EC,¹⁸ leta 2002 pa Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC¹⁹.

Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC, na podlagi katere je bil v Sloveniji sprejet Zakon o elektronskih komunikacijah (ZeKOM)²⁰, je določala, da komunikacij in z njimi povezanih prometnih podatkov ni dovoljeno shranjevati brez soglasja uporabnika, razen za potrebe prenosa ali upravljanja s prometom ter zaračunavanja storitev, oziroma v primeru zakonite sodne odredbe. Izjemo je predstavljalo shranjevanje komunikacij za potrebe dokazovanja komercialnih transakcij, pri čemer pa je direktiva določala, da morajo biti uporabniki predhodno obveščeni o shranjevanju, namenu shranjevanja in trajanju hranjenja, te prometne podatke pa smejo obdelovati samo osebe, ki delujejo pod oblastjo ponudnikov storitev.

Vendar pa so se v Evropi kmalu pojavile ideje o obvezni hrambi prometnih podatkov. V Evropi je do pred kratkim veljalo, da so prometni podatki integralni elementi telefonskih komunikacij (tako je leta 1984 presodilo Evropsko sodišče za človekove pravice v primeru Malone proti Veliki Britaniji²¹), zato naj bi prometni podatki uživali enako stopnjo varstva kot sama vsebina komunikacije oz. naj bi za njihovo beleženje obstajal enak dokazni standard kot za prisluškovanje. Očitno pa se z Direktivo o obvezni hrambi prometnih podatkov²²

arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna preprova uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.« (Klemenčič 2002: 402.)

¹⁷ Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, Mednarodne pogodbe, št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

¹⁸ Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), sprejeta 15. decembra 1997. Official Journal L 024, 30/01/1998 p. 0001 - 0008.

¹⁹ Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

²⁰ Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

²¹ Malone v. Velika Britanija, odločba z dne 2. 8. 1984.

²² Direktiva 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 komunikacij-

to spreminja tudi v Evropi. Potrebno je namreč poudariti, da imajo na prometne podatke v ZDA nekoliko drugačen pogled, saj so leta 1979 v primeru Smith proti Maryland²³ presodili, da prometni podatki o telefonskih pogovorih niso zaščiteni s četrtem amandmajem²⁴ (Turkington in Allen 1999: 104–105)²⁵ s čimer so uvedli ločevanje prometnih podatkov od same vsebine komunikacije. Podobne trende lahko v zadnjem času opazimo tudi v Evropi.

Kljub temu so ideje o obvezni hrambi prometnih podatkov v Evropi naletale na številne kritike, saj se pri tem postavlja načelno vprašanje beleženja osebnih podatkov oseb, ki niso ničesar osumljene ob dejstvu, da je mogoče te podatke kdaj kasneje uporabiti v postopku proti njim. Prvi poskusi v smeri beleženja prometnih podatkov v Evropi segajo v leto 1996, ko je bila v evropskem uradnem listu objavljena Resolucija o zakonitem prestrezanju telekomunikacij (ang. Resolution on the Lawful Interception of Communications). Resolucija je od telekomunikacijskih podjetij v primeru sodne odredbe zahtevala zbiranje velikega števila (osebnih) podatkov, med drugim tudi podatke o lokaciji uporabnika mobilnega telefona. (Council Resolution 1996: 1–6). Leta 1996 je torej Evropska unija določila nabor prometnih podatkov, ki jih telekomunikacijska podjetja morajo beležiti v primeru sodne odredbe. Direktiva o zasebnosti in elektronskih komunikacijah²⁶ iz leta 2002 pa je v 15. členu državam članicam že omogočila hranjenje prometnih podatkov za določen čas. Na podlagi tega člena so imele države članice EU možnost operaterjem mobilne telefonije predpisati rok obveznega hranjenja prometnih podatkov.²⁷ Hraniti so se smeli tudi podatki o lokaciji uporabnika, ki se štejejo med prometne podatke, čeprav nekateri pravni strokovnjaki opozarjajo, da bi t. i. lokacijska zasebnost zaslužila enako pravno varstvo kot sama vsebina komunikacije (Možina 2002: 5).

2. 4 Obvezna hramba prometnih podatkov v EU

Kmalu po sprejemu direktive 2002/58/EC pa so se pojavile ideje o obvezni hrambi prometnih podatkov. EU je pri tem izhajala iz bojazni, da »se zaradi spremembe tehnologije, poslovnih modelov in ponujenih storitev (npr. enotne tarife za uporabo storitev (ang. flat rate), predplačniške in brezplačne elektronske komunikacijske, storitve elektronska pošta, SMS - in MMS - sporočila) ... nekateri prometni podatki ne shranjujejo v takem obsegu kot v preteklih letih. Ti prometni podatki zato niso dostopni oblastem, kadar jih potrebuje.« (DG Information Society and DG Justice and Home Affairs 2004).

skih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

²³ Smith v. Maryland, 242 U.S. 735 (1979).

²⁴ 4. amandma, Listina svoboščin (Bill of Rights), 1791.

²⁵ Četrti amandma ameriške ustave prepoveduje nepooblaščne preiskave in zasege. Leta 1967 je ameriško Vrhovno sodišče v primeru Katz proti Združenim državam (Katz v. United States, 389 U.S. 347 (1967)) presodilo, da četrti amandma ščiti tudi pred prisluškovanjem telefonu brez sodnega naloga in s tem uveljavilo načelo upravičenega pričakovanja zasebnosti (ang. reasonable expectation of privacy).

²⁶ Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.

²⁷ V Sloveniji beleženje lokacije mobilnih telefonov zahteva Pravilnik o programski opremljenosti in vmesnikih za zakonito prestrezanje komunikacij (4. člen, 6. točka), ki je bil 21. marca 2006 objavljen v Uradnem listu RS št. 29/2006.

Sprejemanje direktive so spremljali številni protesti in zapleti, saj sta direktivi nasprotovala tako posebna komisija Evropskega parlamenta (t. i. Alvarova komisija, ki jo je vodil evropski poslanec in poročevalec komiteja evropskega parlamenta za civilne svoboščine, pravosodje in notranje zadeve Alexander Alvaro), ki je predlog zavrnila (Alvaro 2005), kot tudi Evropski parlament. Kljub temu je bila Direktiva o obvezni hrambi prometnih podatkov²²⁸ decembra 2005 sprejeta, aprila 2006 pa tudi objavljena v uradnem listu EU. Če je bilo v prejšnjih direktivah shranjevanje prometnih podatkov prepovedano oziroma dovoljeno le kot izjema, pa je direktiva 2006/24/ES to pravilo povsem obrnila na glavo. Direktiva namreč zahteva obvezno hrambo prometnih podatkov telefonskih in internetnih komunikacij (vključno z naslovi elektronske pošte) ter podatkov o lokacijah mobilnih telefonov, čas hrambe znaša od 6 do 24 mesecev, v nekaterih primerih pa tudi več, poleg tega pa direktiva ne omejuje za katera kazniva dejanja je mogoče shranjene podatke uporabiti.

3.0 Problem hrambe prometnih podatkov

Pri obveznem shranjevanju prometnih podatkov gre za načelno vprašanje beleženja osebnih podatkov oseb, ki niso ničesar osumljene ob dejstvu, da je mogoče te podatke kdaj kasneje uporabiti v postopku proti njim. Dejstvo namreč je, da je mogoče po 149.b in 150. členu Zakona o kazenskem postopku²⁹ prometne podatke pridobiti od operaterjev zgolj na podlagi sodne odredbe v primerih storitve ali priprave hudih kaznivih dejanj. Izjemoma lahko policija po 3. odstavku 149. b člena Zakona o kazenskem postopku³⁰ od operaterja elektronskega komunikacijskega omrežja zahteva, da ji na njeno pisno zahtevo sporoči podatke o lastniku ali uporabniku določenega komunikacijskega sredstva za elektronski komunikacijski promet in o času, v katerem je tako sredstvo bilo oziroma je v uporabi, a le ob podanih razlogih za sum, da je bilo storjeno, oziroma da se pripravlja kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti in je za odkritje tega kaznivega dejanja ali storilca potrebno pridobiti te podatke.

Podobno velja tudi za Slovensko obveščevalno-varnostno agencijo, ki ji lahko predsednik Vrhovnega sodišča Republike Slovenije dovoli nadzorovanje telekomunikacij z izpisom telekomunikacijskega prometa v primeru velike verjetnosti izvajanja ali priprave najhujših kaznivih dejanj (24.a člen Zakona o Slovenski obveščevalno-varnosti agenciji³¹). Tovrsten elektronski nadzor je bil torej do sprejema omenjene direktive mogoč le kot nekakšen skrajni ukrep, uperjen proti osumljencem najhujših kaznivih dejanj. S sprejemom direktive tarče tega ukrepa postajamo vsi uporabniki komunikacijskih sredstev.

Kritiki so tudi mnenja, da je tak ukrep nesorazmeren in da ni nujno potreben v demokratični družbi, zaradi česar je morda v neskladju z Evropsko konvencijo o človekovih pravicah³²

²⁸ Direktiva 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 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

²⁹ Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB3), Uradni list RS, št. 8/2006.

³⁰ Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB3), Uradni list RS, št. 8/2006.

³¹ Zakon o Slovenski obveščevalno-varnosti agenciji (uradno prečiščeno besedilo) (ZSOVA-UPB2), Uradni list RS, št. 81/2006.

³² Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin,

, saj posega tako v pravico do zasebnosti kot tudi v domnevo nedolžnosti. Glavni problem shranjevanja prometnih podatkov o vseh je tako kriminalizacija celotne populacije, saj direktiva ne zahteva zbiranja podatkov o posameznikih, ki so česa osumljeni, pač pa zahteva zbiranje podatkov o vseh. Ravno to odpira vprašanje skladnosti z domnevo nedolžnosti, odpira pa se tudi vprašanje, kako daleč gredo še lahko posegi v zasebnost v imenu varnosti. Če je namreč Evropsko sodišče za človekove pravice leta 1984 v primeru Malone proti Veliki Britaniji³³ zapisalo, da so prometni podatki integralni elementi telefonskih komunikacij (in jih zato sme operater telekomunikacij posredovati državnim organom samo na podlagi sodne odredbe ali pristanka naročnika) (Klemenčič 2002: 403), se lahko ob trenutnem razvoju zakonodajnih ukrepov glede obveznega hranjenja prometnih podatkov vprašamo, ali nas nekoč v prihodnosti ne čaka tudi ukrep, ki bo zahteval obvezno shranjevanje tudi za vsebino telefonskih pogovorov (katere bo operater telekomunikacij dolžan posredovati državnim organom na podlagi sodne odredbe). Na nek način bi torej lahko govorili o sodobnem (elektronskem) panoptikonu. Vzporednice s sprejemanjem zakona Communications Assistance for Law Enforcement Act (CALEA, znan tudi pod imenom Digital Telephony Act),³⁴ v ZDA v začetku 90. let se ponujajo kar same po sebi. Konec 80. let 20. stoletja je ameriški FBI začel izvajati operacijo Root Canal (Operation Root Canal), v okviru katere je telefonske operaterje hotel prepričati, da v svoje telefonske centrale vgradijo tehnične zmožnosti za enostavnejše (oddaljeno) prisluškovanje, hkrati pa bi morali preiskovalnim organom omogočiti tudi dostop do nešifrirane komunikacije v primeru, da se komunikacija šifrira. FBI je tako leta 1991 Kongresu predlagal sprejem določila, ki bi od proizvajalcev in ponudnikov elektronskih komunikacijskih sistemov zahteval, da v svoje proizvode vgradijo tako tehnologijo, ki bo državnim organom omogočila dostop do nešifrirane komunikacije (Phillips 2001: 263). Z drugimi besedami, predlog je predvideval, da bi morali proizvajalci v svoje telefonske centrale vgraditi posebno bližnjico za dostop oziroma t. i. 'stranska vrata' (ang. trap door, back door), skozi katera bi imeli državni organi dostop do telekomunikacijskega omrežja. Zakon je bil kljub kritikam leta 1994 sprejet, kritiki pa so opozarjali, da zakon pomeni pomemben premik v razumevanju pooblastil države. Ne samo da vlada lahko zahteva dostop do komunikacije, pač pa, kot so zapisali predstavniki ACLU v odprtem pismu kongresniku Brooksu 22. septembra 1994, predlog CALEA »ustvarja predpostavko, ki je nevarna in brez primera, da namreč vlada ... lahko od zasebnikov zahteva da ustvarijo poseben dostop (ang. create special access)«. To je po njihovem mnenju primerljivo z »zahtevo, da bi vsi graditelji morali v nove hiše vgraditi nadzorne kamere, ki bi jih lahko uporabljala vlada« (ACLU 1994). Kritika ACLU je bila leta 1994 morda videti kot znanstvena fantastika. Dandanes, ko so nadzorne kamere v nekaterih evropskih mestih že vgrajene v avtobuse, vlake in celo v taksije, pa si je morda že mogoče zamisliti zahtevo, da bi bile v vse hiše vgrajene kamere, ki bi snemale vse dogajanje in posnetke hranile določen čas – posnetki pa bi bili

spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, Mednarodne pogodbe, št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

³³ Malone v. Velika Britanija, odločba z dne 02. 08. 1984.

³⁴ Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

v primeru zakonite zahteve na voljo preiskovalcem.

Poleg preiskovalnih organov imajo velik interes za hrambo in analizo prometnih podatkov tudi operaterji mobilne telefonije in tržniki, saj na njihovi podlagi lažje načrtujejo razvoj omrežja in vlaganja v trženje. Zakonita hramba tovrstnih podatkov je načeloma dovoljena le v primeru, če se podatki hranijo v anonimizirani obliki oziroma če ima operater ustrezno soglasje naročnika. Kljub temu so iz Evrope znani primeri obsežnega zbiranja in hrambe prometnih podatkov brez vednosti naročnikov. Tako je na primer britanski mobilni operater Virgin Mobile leta 2001 priznal, da je hranil prometne in lokacijske podatke uporabnikov za neomejen čas, podatke pa so uporabljali za analizo obremenjenosti omrežja (Wearden 2001). Zanimivo je tudi, da je FBI v ZDA večkrat skušal prepričati operaterje mobilnih komunikacij, da bi mu omogočili lociranje uporabnikov mobilnih telefonov, vendar so podjetja razvoj te tehnologije zavračala z argumentom, da gre za poseg v zasebnost (Etzioni 1999: 130). Potem pa je to tehnologijo začel zahtevati trg, mobilni operaterji pa so zaslutili, da bi bilo mogoče storitev določanja lokacije tržiti in tehnologijo so razvili sami – brez pomoči države. Sredi leta 2006 je drugi največji ponudnik mobilne telefonije v ZDA, podjetje Verizon začelo tržiti storitev sledenja uporabnikom mobilnih telefonov. Sistem je zaenkrat namenjen staršem, ki hočejo spremljati, kje se gibljejo njihovi otroci. Sistem omogoča, da se lokacija mobilnega telefona otroka izriše na zemljevidu (na računalniku ali na mobilni napravi), mogoče pa je nastaviti tudi prostorsko območje, kjer se uporabnik lahko giblje. Če uporabnik območje zapusti, sistem o tem obvesti naročnika storitve z SMS -sporočilom (Reuters 2006).

* * *

Zagovorniki hrambe prometnih podatkov pogosto odgovarjajo, da ne gre za hud poseg v zasebnost, kot je na primer prisluškovanje, ter da so prometni podatki nujni za preganjanje novih oblik kriminala. Vsekakor drži, da je brez prometnih podatkov odkrivanje kakršnegakoli kiberkriminala bistveno oteženo, morda celo nemogoče. Kljub temu pa je mogoče analizo prometnih podatkov uporabiti (zlorabiti) za iskanje vzorcev »sumljivih« dejavnosti ter predvidevanje, kar pomeni hud poseg v človekovo zasebnost in svobodo. Tovrsten podatkovni nadzor je mogoče izvajati v velikem obsegu in povsem nezaznavno, predvsem pa ga je moč avtomatizirati. Prometne podatke je namreč za razliko od prisluhov vsebine glasovne komunikacije mogoče analizirati z metodami izkopavanja podatkov,³⁵ zato hramba prometnih podatkov v mobilni telefoniji predstavlja veliko grožnjo

³⁵ Čeprav je prometne podatke zaradi njihove strukturiranosti mogoče bistveno bolj enostavno analizirati kot vsebino zvočnih komunikacij, pa se premiki kažejo tudi na tem področju. Podjetje Integrated Media Measurement Incorporated je tako od septembra 2005 do aprila 2006 izvedlo meritve izpostavljenosti medijem. Sodelujočim v raziskavi so razdelili posebej prilagojene mobilne telefone, ki so ves čas snemali zvočno okolje in na podlagi posebnih algoritmov izračunavali `fdv_vehovar_mobilne_refleksije_fSec12:254` `Sec12:254` `fdv_vehovar_mobilne_refleksije_fSec12:254` njegove »digitalne prstne odtise« ter jih posredovali na strežnike podjetja (Vavreck, Welsh in Alcorn, 2006: 5-6). Podjetje te vzorce nato primerja z vzorci medijskih vsebin. Predstavniki podjetja trdijo, da je s pomočjo takšnega pasivnega prisluškovanja, ki na vsakih 30 sekund posname in identificira 10 sekund zvočne okolice, mogoče ugotoviti katerim medijskim vsebinam je posameznik izpostavljen in to celo z več kot 99% natančnostjo (IMMI, 2007). Ob tem je zanimivo tudi dejstvo, da je decembra 2006 ameriški okrožni sodnik presodil da je uporaba tim. klateške prisluškovalne naprave (ang. roving bug), ki omogoča prisluškovanje pogovorom, ki se odvijajo v bližini mobilnega telefona osumljenca, zakonita (Kaplan, 2006). Mnenje naj bi bilo posledica dejstva, da je FBI tehniko prisluškovanja s pomočjo prisluškovalne naprave, ki naj bi bila nameščena v mobilni telefon nekega osumljenca že uporabljal. Nekatere analize primera kažejo, da je verjetno, da je FBI preko mobilnega omrežja vključil mikrofona na mobilnem telefonu osumljenca in na tak način prisluškoval pogovorom (Schneier, 2006).

zasebnosti. V nadaljevanju si bomo ogledali dva primera, ki kažeta, kje so možne tovrstne zlorabe.

Julija 2004 je več spletnih medijev poročalo, da se je Kitajska odločila cenzurirati SMS -sporočila v realnem času. Domnevno so se za ukrep odločili, ker ob izbruhu bolezni SARS leta 2003 niso uspeli nadzorovati informacij o širjenju bolezni, čeprav so, kot navajajo poročila, zaradi širjenja t. i. »neresničnih govoric« o SARS-u s pomočjo SMS-sporočil leta 2003 priprli okrog ducat oseb (Richardson 2004). Kot uradni razlog za ta ukrep so navajali preprečevanje pošiljanja goljufivih in obscenih SMS-sporočil. Vendar pa v tem primeru ni problematična le sama cenzura, pač pa predvsem način izvedbe le-te. Kitajska je namreč razvila tehnologijo, ki vsa prestrežena SMS-sporočila pregleda s posebnimi algoritmi, ki iščejo ključne besede ali kombinacije ključnih besed. V primeru, da ključne besede kažejo na kršitev zakonodaje, je o lokaciji mobilnega telefona kršitelja takoj obveščena najbližja policijska postaja (Lim 2004). Kitajski primer kaže na tehnične zmožnosti izvajanja množičnega nadzora v realnem času, velja pa poudariti, da so podobne projekte za zbiranje ter analizo ogromnih količin (prometnih) podatkov financirali tudi v ZDA. Gre za projekte TIA (Terrorist (Total) Information Awareness), LifeLog, CAPPS II (Computer Assisted Passenger Pre-screening System) ter MATRIX (Multistate Anti-Terrorism Information eXchange), ki so bili zaradi pritiskov javnosti ukinjeni, čeprav obstaja sum, da se naskrivaj še vedno razvijajo dalje. Ti sumi so se okrepili predvsem po razkritju, da je NSA – verjetno že sedem mesecev pred terorističnimi napadi 11. septembra 2001 (Harris 2006) – zbirala prometne podatke o telefonskih klicih več deset milijonov Američanov znotraj ZDA ter nad zbranimi podatki izvajala statistične analize (Page 2006). Kmalu za tem razkritjem je prišlo na dan tudi, da ima NSA v Bridgetonu v ZDA, kjer so locirana glavna vozlišča podjetja AT&T za usmerjanje lokalnega in mednarodnega internetnega in telefonskega prometa, v najemu poseben prostor, iz katerega lahko nadzoruje celoten omrežni promet.³⁶ Pred tem je bila razkrita še ena taka lokacija v San Franciscu (Harris 2006). Poleg tega se v zadnjih letih pospešeno razvija tudi področje izkopavanja podatkov (data mining) na področju marketinga, kar pomeni, da se tehnologije, ki omogočajo obsežen podatkovni nadzor, pospešeno razvijajo tako za vladni kot za komercialni sektor. V drugem primeru pa gre za projekt, ki so ga v akademskem letu 2004/2005 izvajali na Massachusetts Institute of Technology v ZDA. V okviru Reality Mining Projecta so s pomočjo posebnega programa, ki so ga namestili na mobilni telefon z operacijskim sistemom Symbian, devet mesecev zajemali podatke o uporabi mobilnih telefonov stotih prostovoljcev. V okviru projekta so beležili podatke o lokaciji mobilnega telefona, komunikaciji (kdo in kako pogosto komunicira s kom) ter bližini ostalih (s pomočjo skeniranja prek povezave Bluetooth). Podatki so razkrili vzorce vsakodnevnega vedenja uporabnikov, analiza podatkov pa je raziskovalcem omogočila da s 85-odstotno natančnostjo predvidijo, kaj bodo uporabniki storili v naslednjem trenutku (MIT 2005 ter Singel 2005). Seveda ni trajalo dolgo, ko se je pojavil tovrsten komercialni izdelek. Aprila 2006 se je namreč pojavil prvi vohunski program za mobilne telefone z operacijskim sistemom Symbian, Flexispy. Vohunski program shranjuje prometne podatke o klicih ter SMS -sporočilih (in vsebini le-teh), podatke pa shranjuje na strežnik podjetja Flexispy. Programa brez posebnega gesla ni mogoče odstraniti (Niemelä in

³⁶ To razkritje za poznavalce ni nič novega, saj ima NSA že tradicijo »sodelovanja« s telekomunikacijskimi podjetji. V letih od 1945 do 1975 je namreč NSA oz. njen predhodnik Black Chamber v ustnem dogovoru z nekaterimi telekomunikacijskimi podjetji prestrezala vsa teleprinterska sporočila. Šlo je za projekt Shamrock (Bamford, 2002: 451–454).

Heikkilä 2006). Podjetje svoj izdelek oglašuje kot pripomoček za zakonske partnerje, ki sumijo, da jih partner vara, ter kot pripomoček za starše, ki bi svoje otroke radi zaščitili pred škodljivimi SMS-sporočili. Naročniki Flexispyevih storitev lahko vsebino prestreženih podatkov pregledujejo prek spletnega vmesnika (Flexispy 2006).

4.0 Obravnava prometnih podatkov v Sloveniji

V Sloveniji je stari Zakon o elektronskih komunikacijah³⁷³⁷ v 104. členu zahteval, da je treba prometne podatke, ki se nanašajo na uporabnike, takoj ko niso več potrebni za prenos sporočil, izbrisati ali spremeniti v brezosebno obliko (razen v primeru pisnega soglasja naročnika, zakonitega prestrezanja komunikacij in do poplčila storitve oz. preteka zastaralnega roka). Po implementaciji vsebine Direktive o obvezni hrambi prometnih podatkov³⁸³⁸ v slovensko zakonodajo decembra 2006, pa je novi Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah³⁹³⁹ v členih 107 do 107. e določil obvezno hrambo prometnih podatkov na področju elektronskih komunikacij. Novi zakon tako določa, da morajo operaterji hraniti podatke potrebne za odkritje in prepoznanje vira in cilja komunikacije, podatke potrebne za ugotovitev datuma, časa in trajanja

komunikacije, podatke potrebne za ugotovitev vrste komunikacije ter podatke potrebne za razpoznavo komunikacijske opreme uporabnikov. Podatki se hranijo za obdobje 24 mesecev od dneva komunikacije. Ti podatki za področje mobilne telefonije med drugim obsegajo kličoče in klicano telefonsko številko, mednarodno identiteto mobilnega naročnika kličoče in klicane stranke, mednarodno identiteto mobilnega terminala kličoče in klicane stranke, v primeru predplačniških anonimnih storitev pa datum in čas začetka uporabe storitve ter ID celice, kjer je bila storitev izvedena (5. odstavek 107. b člena Zakona o spremembah in dopolnitvah Zakona o elektronskih komunikacijah⁴⁰⁴⁰). Za nespoštovanje omenjenih določb so predvidene razmeroma visoke globe, prav tako pa so globe predpisane tudi v primeru hrambe prometnih podatkov za daljši čas, kot ga določa zakon. Pričakovati je, da bodo operaterji komunikacij nove določbe o obvezni hrambi prometnih podatkov spoštovali, postavlja pa se vprašanje ali so spoštovali tudi stare določbe, ki so hrambo prometnih podatkov prepovedovale oz. jo omejevale. V Sloveniji je namreč prišlo do nekaterih dogodkov, ki morda kažejo na to, da operaterji mobilne telefonije teh zakonskih določb v preteklosti niso povsem spoštovali.

Drugega oktobra 2004, tik pred nastopom volilnega molka, je operater Simobil poslal večje število naročenih politično-reklamnih SMS -sporočil. Zaradi tehničnih težav, ki jih je povzročila nevihta (to je pokazala kasnejša preiskava), je okrog 70.000 uporabnikov podjetja Mobitel sporočila dobilo po polnoči, torej v času predvolilnega molka. Med prejemniki je seveda ta dogodek povzročil veliko

³⁷ Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

³⁸ Direktiva 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 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

³⁹ Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-A), Uradni list RS, št. 129/06.

⁴⁰ Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-A), Uradni list RS, št. 129/06.

razburjenje, zato so pričeli množično klicati Mobitelov center za pomoč uporabnikom. Mobitel je zato svojim 70.000 uporabnikom, ki so sporočila prejeli po polnoči, poslal opravičilo oz. pojasnilo (Kovačič 2004).

Vprašanje, ki se zastavlja, pa je, kako so pri Mobitelu vedeli, kdo so bili prejemniki sporočila po polnoči. Kot kaže, je to tehnično mogoče le s shranjevanjem vsebine sporočil ali pa prometnih podatkov. Pri Mobitelu so zanikali, da bi beležili

vsebine SMS -sporočil, posredno pa so potrdili, da so zabeležili številko pošiljatelja SMS-sporočila (torej prometni podatek): »V družbi Mobitel smo v skrbi za naše uporabnike in z namenom zagotavljanja učinkovite pomoči našim uporabnikom morali reagirati in poslati obvestilo s pojasnilom uporabnikom, ki so prejeli SMS iz Simobilovega strežnika (iz številke 94420390) po polnoči iz petka na soboto, ko je začelo veljati pravilo volilnega molka.« (Mobitel 2004). Na eksplicitno vprašanje glede časa hrambe prometnih podatkov o prejemnikih in pošiljateljih SMS-sporočil so pri Mobitelu odgovorili, da se »podatki o poslanih in prejetih SMS-ih (številki pošiljatelja in čas pošiljanja ter številka prejemnika in čas prejema) v skladu z določilom 1. odstavka 104. člena ZEK-a takoj po opravljenem prenosu spremenijo v brezosebno obliko, hranimo pa jih za zakonsko opredeljene potrebe (npr. obračun ali za primere, če naši uporabniki pisno zahtevajo, da izsledimo zanje zlonamerne ali moteče klice – 7. odstavek 105. člena ZEK-a).« (Mobitel 2004).

Ob tem se seveda postavlja vprašanje, kako so pri mobilnem operaterju vedeli, kdo so bili prejemniki spornih SMS-sporočil (ki so jim poslali omenjeno pojasnilo), če pa se prometni podatki takoj po prenosu spremenijo v brezosebno obliko.

Drugi dogodek, ki razkriva kakšne prometne podatke operaterji mobilne telefonije lahko beležijo, pa je sodna obravnava na Okrožnem sodišču v Kranju iz junija 2004. Na obravnavi, na kateri so obtoženim sodili zaradi tatvine avtomobilov, je tožilstvo predstavilo izpiske odhodnih in dohodnih klicev obtožencev skupaj z lokacijami baznih celic. Na podlagi tega je tožilstvo pripravilo zemljevid lokacij in gibanja obtoženih, kar je bila tudi podlaga za obsodbo. Iz zapisnika glavne obravnave v spisu K 74/2003⁴¹

iz dne 26. 9. 2003 je iz pričanj

Simobilovega in Mobitelovega tehnika mogoče razbrati, da so slovenski operaterji mobilne telefonije tehnično sposobni hraniti podatke o vsaj grobih lokacijah uporabnikov mobilnih telefonov. Eden izmed tehnikov je takole izpovedal na sodišču:

»Priča: V zvezi z vprašanjem zagovornika obtoženega ***** povem, da ima podjetje Vega (WWI) nekaj lastnih baznih postaj s svojimi baznimi celicami. Sicer pa gostujejo pri Mobitelu d. d. in uporabljajo torej naše bazne celice in v primeru, da bi naslovili podjetju Vega zahtevek, da vam posreduje izpis odhodno dohodnih klicev z navedbo baznih postaj in baznih celic, so to dolžni posredovati.

Tožilec: Po lastnem vedenju za operaterja mobilne telefonije Vega posreduje izpis odhodno dohodnih klicev, vendar pa ne izpis baznih postaj in baznih celic.

Priča ***** nadaljujem, da podjetje Vega takrat, kadar koristi Mobitelove bazne celice dobi od Mobitela tudi izpisek baznih celic, in v kolikor se takšen izpis baznih celic zahteva, ocenjujem, da ga je Vega sposobna narediti. Ali imajo ustrezno orodje ne vem, več ali manj pa posredujemo Vega

⁴¹ List. št. 2712–2717 ter list. št. 2738–2743.

tovrstne informacije .« (Okrožno sodišče v Kranju 2003). »Po 1. odstavku 130. člena Ztel so bili operaterji dolžni, kadar je to v skladu z ZKP, sodišču sporočiti podatke o udeležencih, sporočilih, okoliščinah in dejstvih telekomunikacijskega prometa za posamezne primere na način, v obsegu in trajanju, kot je določila odredba pristojnega sodišča. V naslednjem členu pa so bili naštetí prometni podatki , ki se nanašajo na naročnika in uporabnika in so potrebni za vzpostavljanje zveze, ki jih je operater lahko hranil in obdeloval in pogoji, ki jih pri tem moral upoštevati. Med temi evidentiranje klicev po baznih postajah ni bilo izrecno navedeno. Vendar pa je to samo po sebi umevno, saj nekaterih podatkov (primeroma tistih iz 1. 2. 4. in 5. točke) praktično ni mogoče evidentirati, ne da bi bilo razvidno, katera bazna postaja je klic zabeležila. Zgolj tak samodejni mehanični izpis klica še ne pomeni poseganja v ustavno zagotovljeno pravico do zasebnosti, marveč je ta lahko prekršena le v primeru nezakonite obdelave takega podatka. Zato je napačno stališče zahteve, da mobilni operaterji z evidentiranjem pogovorov po baznih postajah zbirajo podatke o gibanju svojih strank. Na ta način evidentirajo le telefonske povezave, ki jih vzpostavljajo imetniki mobilnih telefonov, pri čemer drži, da je eden od elementov za ugotavljanje gibanja posameznega obsojenca morebitna uporaba mobilnega telefona na določenem območju, kjer deluje bazna postaja.« (Odločba Vrhovnega sodišča RS, št. I Ips 264/2005 ter št. I Ips 292/2004)

Podobno je moč razbrati tudi iz odločitve Vrhovnega sodišča I Ips 292/2004, I Ips 264/2005

Tedaj veljavni Zakon o varstvu osebnih podatkov⁴² je v 3. točki 1. člena določal da »obdelava osebnih podatkov pomeni zbiranje, shranjevanje ali združevanje podatkov v zbirkah osebnih podatkov, spreminjanje, uporabo ali sporočanje, vključno s prenosom, iskanjem, blokiranjem in brisanjem; obdelava je lahko ročna ali s sredstvi informacijske tehnologije« (podobno definicijo ima tudi 6. člen ZVOP-1⁴³). Glede na to bi lahko zaključili, da samodejni mehanični izpis bazne postaje pomeni poseg v ustavno zagotovljeno pravico do zasebnosti, kadar mobilni operater ta podatek nezakonito obdeluje – torej nezakonito shrani, nezakonito uporabi ali nezakonito (komu) sporoči. Kdaj torej »evidentiranje pogovorov po baznih postajah« ni zakonito?

Kot že rečeno, tedaj veljavni Zakon o elektronskih komunikacijah⁴⁴ je v 104. členu zahteval, da je prometne podatke, ki se nanašajo na uporabnike, treba – takoj ko niso več potrebni za prenos sporočil – izbrisati ali spremeniti v brezosebno obliko. Pred njim veljavni Zakon o telekomunikacijah⁴⁵ je podobno v 131. členu zahteval, da: »... prometne podatke, ki se nanašajo na naročnika in uporabnika in so potrebni za vzpostavljanje zveze, lahko operater hrani in obdeluje toliko časa, dokler traja zveza. Po končani zvezi jih mora operater zbrisati ali spremeniti tako, da se ne nanašajo na konkretno pravno ali fizično osebo.« Izjema od tega pravila je bila mogoča za potrebe obračunavanja, ko je lahko operater do plačila storitve, preteka zakonitega zastaralnega roka, pravnomočne odločbe o terjatvi v

⁴² Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 59/1999, 57/2001 (59/2001 - popr.), 73/2004-ZUP-C, 86/2004-ZVOP-1), ne velja od: 1. 1. 2005.

⁴³ Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/2004 in 113/2005.

⁴⁴ Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.

⁴⁵ Zakon o telekomunikacijah (ZTel), Uradni list RS, št. 30/01, 52/02-ZJA, 110/02-ZGO-1 in 43/04-ZEKom, ne velja od : 1. 5. 2004.

primeru spora ali odredbe sodišča te podatke hranil.

Vrhovno sodišče je bilo v odločbi I Ips 292/2004, I Ips 264/2005 mnenja, da nekaterih prometnih podatkov, katerih zbiranje zakon dovoljuje (konkretno podatkov iz 2. odstavka 131. člena: številko ali identifikacijo kličočega in klicanega, naslov naročnika in tip terminala, skupno število obračunskih enot v obračunani periodi ter vrsto datum, čas in trajanje klica oziroma količine prenesenih podatkov), »praktično ni mogoče evidentirati, ne da bi bilo razvidno katera bazna postaja je klic zabeležila«. Iz tega je mogoče sklepati, da bazna postaja samodejno sporoča nabor prometnih podatkov, katerega del operater potrebuje za potrebe obračunavanja. V tem paketu so očitno tudi lokacijski podatki.

Postavlja se torej vprašanje, ali so operaterji te (dodatne) podatke tudi hranili (torej obdelovali) v zbirki osebnih podatkov. Iz omenjene odločbe Vrhovnega sodišča RS lahko sklepamo, da je vsaj v nekaterih primerih bilo tako. Iz zapisnika glavne obravnave v spisu K 74/2003 pa je moč razbrati, da vsaj eden od treh slovenskih operaterjev mobilne telefonije (Vega) lokacijskih podatkov tožilstvu v preteklosti ni posredoval (kljub temu da po pričanju Mobitelovega tehnika Mobitel tovrstne podatke Vega posreduje, kadar Vega uporablja Mobitelove bazne postaje). Glede na to da so operaterji na zahtevo sodišča te podatke dolžni posredovati, lahko sklepamo, da Vega teh podatkov ni imela, torej jih verjetno ni shranjevala, čeprav jih je dobila »v paketu«.

Podobnega mnenja, namreč da gre pri beleženju lokacijskih podatkov za beleženje »v paketu«, pa je bil tudi mobilni operater Mobitel v odgovoru na vprašanje ob dogodku s pošiljanjem SMS -sporočil oktobra 2004. Na vprašanje, ali podjetje Mobitel beleži in hrani lokacije uporabnikov mobilnih telefonov, so odgovorili: »Mobitel beleži in za zakonsko opredeljene potrebe hrani t. i. prometne podatke, katerih del je tudi podatek o bazni postaji, preko katere je bil opravljen klic ali katera od drugih mobilnih storitev. Pooblaščen organi imajo lahko na podlagi odredbe pristojnega organa, če ta tako zahteva, dostop do teh podatkov.« (Mobitel 2004). Iz odgovora je mogoče razumeti, da so pri Mobitelu mnenja, da so lokacijski podatki del prometnih podatkov, ki jih je operater dolžan hraniti za potrebe obračunavanja (oziroma druge zakonsko opredeljene potrebe). Vendar pa mobilni operaterji lokacijskih podatkov ne potrebujejo za obračunavanje storitev. Kot verjetno kaže primer operaterja Vega in glede na značilnosti sodobnih baz podatkov, pa je jasno, da je nepotrebne ali nezaželene podatke iz »paketa podatkov« mogoče tudi zavreči. Vprašanje je namreč, ali shranjevanje nepotrebni podatkov v tem primeru ne predstavlja kršenje načela nesorazmernosti oz. ali takšno zbiranje osebnih podatkov ni prekomerno, kar glede obdelave osebnih podatkov zakonodaja s tega področja prepoveduje.

5.0 Sklep

Vsekakor velja, da posameznik v zvezi s prometnimi podatki in z vsebino komunikacije upravičeno pričakuje zasebnost. Prometni podatki namreč kažejo na lastnosti komunikacije. Takemu stališču pritruje tudi evropska pravna praksa. Po drugi strani pa sodobna tehnologija omogoča zbiranje in analizo prometnih podatkov v velikem obsegu. Kot je bilo prikazano, je takšne podatke že mogoče uporabiti za namene množičnega nadzora. Te tehnične zmožnosti pa pri državnih organih vzbujajo številne apetite – če je bilo zbiranje prometnih podatkov

brez utemeljenega razloga ali soglasja posameznika v preteklosti izrecno prepovedano, je z Direktivo o obvezni hrambi prometnih podatkov⁴⁶ tak nadzor postal obvezen. To pa za pravico do zasebnosti posameznikov pomeni velike spremembe. Pravica do zasebnosti na področju telekomunikacij je pomembna predvsem zaradi svobodne in nenadzorovane izmenjave sporočil, mnenj in informacij med posamezniki, kar je tudi temelj svobodne in demokratične družbe. Glede na to da ima praktično vsak prebivalec razvitega zahodnega sveta svoj mobilni telefon in da je mobilni telefon danes eno najpomembnejših komunikacijskih sredstev, je grožnja mobilni zasebnosti morda resnejša, kot si povprečni uporabnik mobilnega telefona danes sploh predstavlja.

6.0 Viri in literatura

- [1.] ACLU (1994): ACLU Opposes FBI Wiretap Access Bill Legislation Would Create Dangerous Precedent. Sporočilo za javnost iz dne 26. septembra 1994. Dostopno na: <http://www.eff.org/Legislation/Bills_by_number/hr4922_94_aclu.analysis>. (Datum dostopa: 17. 5. 2004).
- [2.] Agre E. P., in Rotenberg M. (Ur.) (2001): Technology and Privacy: The New Landscape. Cambridge, Massachusetts, London, England: MIT Press.
- [3.] Alvaro, A. N. (2005): Draft report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004 – C6-0198/2004 – 2004/0813(CNS)). Committee on Civil Liberties, Justice and Home Affairs, 18. 4. 2005. Dostopno na: <<http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf>>. (Datum dostopa: 24. oktober 2005).
- [4.] Bamford, J. (2002): Body of Secrets. ZDA: Anchor Books.
- [5.] Bennett J. C. (2001): »Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?«. V E. P. Agre in Rotenberg, M. (Ur.): Technology and Privacy: The New Landscape, 99–123. Cambridge, Massachusetts, London, England: MIT Press.
- [6.] Cate, H. F. (1997): Privacy in the Information Age. Washington: Brookings Institution Press.
- [7.] Čebulj, J. (1992): Varstvo informacijske zasebnosti v Evropi in Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti v Ljubljani.
- [8.] Deleuze, G. (2002): Družba nadzora. Filozofski vestnik, 3, letnik XXIII, 167-177. Ljubljana: Filozofski inštitut ZRC SAZU.
- [9.] DG Information Society and DG Justice and Home Affairs (2004): DG INFSO - DG JAI consultation document on traffic data retention. Delovni dokument, 30. julij 2004. Dostopno na: <http://europa.eu.int/information_society/topics/ecom/doc/useful_information/library/public_consult/data_retention/consultation_data_retention_30_7_04.pdf> (Datum dostopa: 26. 5. 2004).

⁴⁶ Direktiva 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 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

- 10.] Etzioni, A. (1999): The Limits of Privacy. ZDA: Basic Books.
 - 11.] Flexispy . (2006): Spletna stran podjetja Flexispy. <<http://www.flexispy.com/>>. (Datum dostopa: 8. maj 2006).
 - 12.] Foucault , M. (1984): Nadzorovanje in kaznovanje. Delavska enotnost: Ljubljana.
 - 13.] Foucault , M. [Dolar Mladen (ur.)] (1991): Vednost - oblast - subjekt. Krt: Ljubljana.
 - 14.] Foucault , M. (1997/2003): »Predavanje 17. marca 1976«. Filozofski vestnik, 3, letnik XXIV, 151–169. Ljubljana: Filozofski inštitut ZRC SAZU.
 - 15.] Harris, A. (2006): Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say. Bloomberg.com, 30. junij 2006. Dostopno na: <<http://www.bloomberg.com/apps/news?pid=20601087&sid=abIV0cO64zJE&refer=#>> (Datum dostopa: 3. julij 2006).
 - [16.] IMMI 2007. Data Collection. <<http://www.immi.com/dataClctn.html>>. (Datum dostopa 23. februar 2007).
 - [17.] Kaplan, L. A. (2006). Memorandum Opinion. Mnenje Okrožnega sodnika Lewisa A. Kaplana iz dne 27. novembra 2006 v primeru United States of America v. John Tomero, in dr., No. S2 06 Crim. 0008(LAK).United States District Court, S.D: New York. Kopija dokumenta je dostopna na: <<http://www.politechbot.com/docs/fbi.ardito.roving.bug.opinion.120106.txt>>. (Datum dostopa: 6. december 2006).
 - [18.] Klemenčič, G. (2002): 37. člen (varstvo tajnosti pisem in drugih občil). V L. Šturm (ur.) 2002: Komentar ustave republike Slovenije, 391-408. Ljubljana: Fakulteta za podiplomske državne in evropske študije.
 - [19.] Kovačič , M. (2004): Zakoniti nadzor v Sloveniji (2. del). Slo-Tech, 28. oktober 2004. <<http://www.slo-tech.com/clanki/04020/>>. (Datum dostopa: 28. oktober 2004).
 - [20.] Lampe, R. (2004): Sistem pravice do zasebnosti. Ljubljana: Bonex založba.
 - [21.] Laurant, C. (ur.) (2003): Privacy & Human Rights. ZDA: EPIC in Privacy International.
 - [22.] Lim, L. (2004): China to censor text messages. BBC News. 2. julij 2004. <<http://news.bbc.co.uk/1/hi/world/asia-pacific/3859403.stm>> (Datum dostopa: 23. 11. 2004).
 - [23.] MIT 2005. Reality Mining Project. <<http://reality.media.mit.edu/>> (Datum dostopa: 8. maj 2006).
 - [24.] Mobitel (2004): Odgovor Mobitelove Službe za odnose z javnostmi na moja vprašanja, 19. oktober 2004. Elektronsko sporočilo poslano iz naslova <PRMobitel@mobitel.si>, dne 19. oktobra 2004 ob 18:41:18.
 - [25.] Možina, D. (2002): Se Evropa odreja zasebnosti v korist varnosti?. Informatika in pravo, (1): 3–5, priloga Pravne prakse, št 43. Ljubljana: Gospodarski vestnik.
 - [26.]
- Niemelä, J. in Heikkilä, J. (2006): F-Secure Trojan Information Pages: Flexispy .A. F-Secure, 29. marec 2006. <http://www.f-secure.com/v-descs/flexispy_a.shtml>. (Datum dostopa: 8. maj 2006).
- [27.] Okrožno sodišče v Kranju (2003): Del zapisnika glavne obravnave v kazenski zadevi, opr. št. K 74/2003 pred Okrožnim sodiščem v Kranju, list št. 2712 - 2717 ter list št. 2738 - 2743.
- Dokument je bil maja 2006 na podlagi Zakona o dostopu do informacij javnega značaja pridobljen od Vrhovnega sodišča RS, št. Su 36-03/2006 – 78 – 2.
- [28.] Page, S. (2006): NSA secret database report triggers fierce debate in Washington. USA Today, 11. maj 2006. <http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.

htm> (Datum dostopa: 3. julij 2006).

[29.] Perenič, A. (ur.) (1979): Zbornik znanstvenih razprav. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.

[30.] Phillips, J. D. (2001): Cryptography, Secrets, and the Structuring of Trust. V Agre E. P. in Rotenberg M., (ur.) (2001): Technology and Privacy: The New Landscape, 243–276. Cambridge, Massachusetts, London, England: MIT Press.

[31.] Reuters. (2006): Verizon to launch mobile chaperone service. ZDNet, 10. junij 2006. <[http://](http://news.zdnet.com/2100-1040_22-6082472.html)

news.zdnet.com/2100-1040_22-6082472.html> (Datum dostopa: 11. 11. 2006).

[32.] Richardson, T. (2004): China snoops on text messages. The Register, 2. julij 2004. <[http://](http://www.theregister.co.uk/2004/07/02/china_text_snoop/)

www.theregister.co.uk/2004/07/02/china_text_snoop/>. (Datum dostopa: 23. 11. 2004).

[33.] Schneier, B. (2006). Remotely Eavesdropping on Cell Phone Microphones. Schneier.com, 5.

december 2006. <http://www.schneier.com/blog/archives/2006/12/remotely_eavesd.html>. (Datum dostopa: 6. december 2006).

[34.] Singel, R. (2005): When Cell Phones Become Oracles. Wired, 25. julij 2005. <[http://www.](http://www.wired.com/news/wireless/0,1382,68263,00.html)

[wired.com/news/wireless/0,1382,68263,00.html](http://www.wired.com/news/wireless/0,1382,68263,00.html)> (Datum dostopa: 8. maj 2006).

[35.] Šelih, A. (1979): Zasebnost in nove oblike njenega kazenskopravnega varstva. V A. Perenič

(ur.) (1979): Zbornik znanstvenih razprav, 39, 1979, 149–181. Ljubljana: Univerza v Ljubljani, Pravna fakulteta.

[36.] Temporary Committee on the ECHELON Interception System (2001): Working document in

preparation for a report on the existence of a global system for intercepting private and commercial communications (ECHELON interception system). European Parliament.

[Dostopno na: <http://www.fas.org/irp/program/process/euoparl_draft.pdf>. (Datum dostopa: 1. 4. 2004).]

[37.] Turkington, C. R., in Allen, L. A. (1999): Privacy Law : Cases and Materials. ZDA: West Group.

[38.] Vavreck, L., Welsh, A. in Alcorn, A. (2006). Closing the Marketing Loop: Measuring Real World Clickthrough and Conversion for King Kong. Advertising Research Foundation Conference on Audience Measurement, 20-21 junij 2006, New York: New York.

<<http://www.immi.com/images/ARF68V6.pdf>>. (Datum dostopa: 20. februar 2007).

[39.] Wagner DeCew, J. (1997): In Pursuit of Privacy. Ithaca, London: Cornell University Press.

[40.] Wearden, G. (2001): Virgin Mobile admits storing customer location records. ZDNet, 29. oktober 2001.

[41.] <<http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2098193,00.htm>>. (Datum dostopa: 5. maj 2006).

[42.] Whitaker, R.. (1999): The End of Privacy. New York: The New Press.

[43.] White, C. J. (2003): People, Not Places – A Policy Framework for Analyzing Location Privacy Issues. EPIC. <<http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf>>.

(Datum

dostopa: 1. 4. 2004).

6. 1 Slovenski pravni dokumenti

- [1.] Odločba Vrhovnega sodišča RS, št. I Ips 264/2005, št. I Ips 292/2004. Dokument je bil maja 2006 na podlagi Zakona o dostopu do informacij javnega značaja pridobljen od Vrhovnega sodišča RS, št. Su 36-03/2006 – 78 – 2.
- [2.] Pravilnik o programski opremi in vmesnikih za zakonito prestrezanje komunikacij, Uradni list RS, št. 29/2006.
- [3.] Zakon o elektronskih komunikacijah (ZeKOM), Uradni list RS, št. 43/04 in 86/04 – ZVOP-1.
- [4.] Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-A), Uradni list RS, št. 129/06.
- [5.] Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB3), Uradni list RS, št. 8/2006.
- [6.] Zakon o Slovenski obveščevalno-varnostni agenciji (uradno prečiščeno besedilo) (ZSOVA-UPB2), Uradni list RS, št. 81/2006.
- [7.] Zakon o telekomunikacijah (ZTel), Uradni list RS, št. 30/01, 52/02-ZJA, 110/02-ZGO-1 in 43/04-ZEKom.
- [8.] Zakon o varstvu osebnih podatkov (ZVOP), Uradni list RS, št. 59/1999, 57/2001 (59/2001 - popr.), 73/2004-ZUP-C, 86/2004-ZVOP-1), ne velja od: 1. 1. 2005.
- [9.] Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

6. 2 Odločitve Evropskega sodišča za človekove pravice

- [1.] Copland v. Velika Britanija, odločba z dne 3. 4. 2007.
- [2.] Halford v. Velika Britanija, odločba z dne 25. 6. 1997.
- [3.] Klaas et. al v. ZR Nemčija, odločba z dne 6. 9. 1978.
- [4.] Kopp v. Švica, odločba z dne 25. 3. 1998.
- [5.] Lambert v. Francija, odločba z dne 24. 8. 1998.
- [6.] Malone v. Velika Britanija, odločba z dne 2. 8. 1984.
- [7.] Niemietz v. ZR Nemčija, odločba z dne 16. 12. 1992.

6. 3 Dokumenti EU

- [1.] Direktiva 95/46/EC o varstvu posameznikov pri obdelovanju osebnih podatkov in svobodnem pretoku teh podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), sprejeta 24. oktobra 1995. Official Journal L 281, 23/11/1995 p. 0031 - 0050.
- [2.] Direktiva 97/66/EC o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacij-skem sektorju (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector), sprejeta 15. decembra 1997. Official Journal L 024, 30/01/1998 p. 0001 - 0008.
- [3.] Direktiva 2002/58/EC o obdelovanju osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector), sprejeta 12. julija 2002. Official Journal L 201, 31/07/2002 p. 0037 - 0047.
- [4.] Direktiva 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 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications

networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 – 0063. [5.] Resolucija o zakonitem prestrezanju telekomunikacij (Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications), sprejeta 17. januarja 1995. Official Journal, C 329, 4. 11. 1996, p. 1–6.

6. 4 Dokumenti OECD

[1.] OECD. 1980. Smernice za zaščito zasebnosti in čezmejni pretok osebnih podatkov (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), sprejete 23. septembra 1980.

6. 5 Dokumenti Sveta Evrope

[1.] Svet Evrope. 1950. Evropska konvencija o varstvu človekovih pravic in mednarodnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 3, 5 and 8 and amended by Protocol No. 2 and its Protocols Nos. 1, 4, 6, 7, 9, 10 and 11), sprejel jo je Svet Evrope leta 1950. Uradni list RS, št. 33/1994, Mednarodne pogodbe, št. 7/1994, 13. 6. 1994. Konvencijo je Državni zbor Republike Slovenije ratificiral 13. 6. 1994. Veljati je začela dne 28. 6. 1994.

[2.] Svet Evrope. 1981. Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Convention for the Protection of Individuals with Automatic Processing of Personal Data), sprejel jo je Svet Evrope 28. 1. 1981. Uradni list RS, Mednarodne pogodbe, št. 3/1994. Konvencijo je Državni zbor Republike Slovenije ratificiral dne 25. 1. 1994. Veljati je začela dne 1. 3. 1994.

6. 6 Zakonodaja ZDA266

[1.] Ustava Združenih držav Amerike (C

[2.] Listina svoboščin (Bill of Rights), 179

var_mobilne_refleksije_fSec12:266 Sec12:266 var_mobilne_refleksije_fSec12:266 Sec12:
[3.] Communications Assistance for Law Enforcement Act (Digital Telephony Act) of 1994, 47 U.S.C. (1994).

6. 7 Odločitve Vrhovnega sodišča ZDA

[1.] Katz v. United States, 389 U.S. 347 (1967).

[2.] Smith v. Maryland, 442 U.S. 735 (1979).

[3.] U.S. West v. F.C.C., 182 F.3d 1224 (1999).