



Mediji in informacije

Sodišče Evropske unije  
**SPOROČILO ZA MEDIJE ŠT. 145/16**

Luxembourg, 21. december 2016

Sodba v združenih zadevah C-203/15 Tele2 Sverige AB/ Post-och telestyrelsen in C-698/15 Secretary of State for the Home Department/Tom Watson in drugi

## **Države članice ponudnikom elektronskih komunikacijskih storitev ne smejo naložiti splošne obveznosti hrambe podatkov**

*Pravo Unije nasprotuje splošni in neselektivni hrambi podatkov o prometu in podatkov o lokaciji, vendar smejo države članice določiti preventivno ciljno hrambo teh podatkov z edinim namenom boja proti hudemu kriminalu, če se taka hramba glede kategorij hranjenih podatkov, uporabljenih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe, omeji le na to, kar je nujno potrebno. Za dostop nacionalnih organov do hranjenih podatkov je treba določiti nekatere pogoje, med katerimi sta predhodni nadzor neodvisnega organa in hramba podatkov na ozemlju Unije*

Sodišče je v sodbi Digital Rights Ireland iz leta 2014<sup>1</sup> Direktivo o hrambi podatkov<sup>2</sup> razglasilo za neveljavno, ker splošna obveznost hrambe podatkov o prometu in podatkov o lokaciji, ki jo ta direktiva določa, pomeni poseg v temeljni pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov, ki ni omejen na najnujnejše.

Po izdaji te sodbe je Sodišče prejelo v odločanje dve zadevi, ki se nanašata na splošno obveznost na Švedskem in v Združenem kraljestvu, da ponudniki elektronskih komunikacijskih storitev hranijo podatke v zvezi s temi komunikacijami, katerih hramba je bila določena z direktivo, razglašeno za neveljavno.

Dan po izreku sodbe Digital Rights Ireland je telekomunikacijsko podjetje, družba Tele2 Sverige, švedski regulativni organ za pošto in telekomunikacije obvestilo o svoji odločitvi, da bo prenehalo hraniti podatke in da namerava že registrirane podatke izbrisati (zadeva C-203/15). Švedsko pravo namreč ponudnikom elektronskih komunikacijskih storitev nalaga, da sistematično, kontinuirano in brez kakršnekoli izjeme hranijo vse podatke o prometu in podatke o lokaciji za vse svoje naročnike in registrirane uporabnike glede vseh elektronskih komunikacijskih sredstev.

V zadevi C-698/15 so Tom Watson, Peter Brice in Geoffrey Lewis vložili tožbe zoper britansko ureditev hrambe podatkov, na podlagi katere lahko minister za notranje zadeve javnim telekomunikacijskim operaterjem določi obveznost hrambe vseh podatkov v zvezi s komunikacijami za največ dvanajst mesecev, pri tem pa je izključena hramba vsebine teh komunikacij.

Na podlagi predloga Kammarrätten i Stockholm (pritožbeno upravno sodišče v Stockholmu, Švedska) in predloga Court of Appeal (England and Wales) (Civil Division) (civilni oddelek pritožbenega sodišča Anglije in Walesa, Združeno kraljestvo) je Sodišče pozvano, naj ugotovi, ali sta nacionalni ureditvi, ki ponudnikom nalagata splošno obveznost hrambe podatkov in ki določata dostop pristojnih nacionalnih organov do hranjenih podatkov, ne da bi ta dostop omejevali zgolj za namene boja proti hudemu kriminalu in za dostop določili pogoj predhodnega nadzora s strani

<sup>1</sup> Sodba Sodišča z dne 8. aprila 2014, *Digital Rights Ireland in Seitlinger in drugi* (združeni zadevi [C-293/12 in C-594/12](#), glej [SM št. 54/14](#)).

<sup>2</sup> 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 (UL L 105, str. 54).

sodišča ali neodvisnega upravnega organa, v skladu s pravom Unije (v tem primeru z Direktivo o zasebnosti in elektronskih komunikacijah<sup>3</sup> glede na Listino Evropske unije o temeljnih pravicah<sup>4</sup>).

V današnji sodbi **Sodišče odgovarja, da pravo Unije nasprotuje nacionalni ureditvi, ki določa splošno in neselektivno hrambo podatkov.**

Sodišče najprej potrjuje, da zadevni **nacionalni ukrepi spadajo na področje uporabe Direktive**. Varstvo zaupnosti elektronskih komunikacij in podatkov o prometu, ki ga zagotavlja Direktiva, se namreč uporablja za ukrepe, ki so jih sprejele vse osebe razen uporabnikov, ne glede na to, ali gre za zasebne osebe ali subjekte ali državne organe.

Sodišče dalje ugotavlja, da čeprav ta direktiva državam članicam dopušča, da omejijo obseg načelne obveznosti zagotavljanja zaupnosti komunikacij in z njimi povezanimi podatki o prometu, ne more upravičiti tega, da odstopanje o te načelne obveznosti in zlasti od prepovedi hrambe teh podatkov, ki je določeno z njo, postane pravilo.

Poleg tega Sodišče opozarja na svojo ustaljeno sodno prakso, v skladu s katero varstvo temeljne pravice do spoštovanja zasebnega življenja zahteva, da se **odstopanja** od varstva osebnih podatkov **določijo v mejah tega, kar je nujno potrebno**. Sodišče to sodno prakso uporabi za pravila, ki urejajo hrambo podatkov, in za pravila, ki urejajo dostop do hranjenih podatkov.

Sodišče **v zvezi s hrambo** ugotavlja, da je na podlagi vseh teh hranjenih podatkov **mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb**, katerih podatki so bili hranjeni.

**Poseg, ki izhaja iz nacionalne ureditve, ki določa hrambo podatkov o prometu in podatkov o lokaciji, je treba obravnavati kot zelo resnega**. Okoliščina, da se hramba podatkov izvede, ne da bi bili uporabniki elektronskih komunikacijskih storitev o tem obveščeni, lahko pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje. Zato **lahko le boj proti hudemu kriminalu upraviči ta ukrep**.

Sodišče navaja, da **ureditev, ki določa splošno in neselektivno hrambo podatkov, ne zahteva povezave med podatki, za katere se določa hramba, in grožnjo za javno varnost** in predvsem ni omejena na hrambo podatkov v zvezi z začasnim obdobjem in/ali geografskim območjem in/ali krogom oseb, ki so lahko vpletene v hudo kaznivo dejanje. **Taka nacionalna ureditev torej presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva Direktiva glede na Listino**.

Sodišče, nasprotno, pojasnjuje, da **Direktiva ne nasprotuje nacionalni ureditvi, ki določa ciljno hrambo podatkov** za namene boja proti hudemu kriminalu, **če se taka hramba** glede kategorij hranjenih podatkov, uporabljenih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe **omeji le na to, kar je nujno potrebno**. Po mnenju Sodišča **mora biti vsaka nacionalna ureditev, ki to predvideva, jasna in natančna in mora določiti zadostna jamstva**, da se podatki zavarujejo pred tveganjem zlorabe. Določiti mora okoliščine in pogoje, pod katerimi je mogoče preventivno sprejeti ukrep o hrambi podatkov, da se zagotovi, da je obseg tega ukrepa v praksi dejansko omejen na tisto, kar je nujno potrebno. Zlasti mora taka ureditev **temeljiti na objektivnih elementih**, na podlagi katerih je mogoče opredeliti osebe, katerih podatki bi lahko izkazovali zvezo s hudimi kaznivimi dejanji, prispevati k boju proti hudemu kriminalu ali preprečiti resno nevarnost za javno varnost.

Glede **dostopa pristojnih nacionalnih organov do hranjenih podatkov** Sodišče potrjuje, da se zadevna nacionalna ureditev ne sme omejiti le na to, da zahteva, da dostop ustreza kateremu od ciljev iz Direktive, čeprav gre za boj proti hudemu kriminalu, temveč mora določiti tudi vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov. Ta

<sup>3</sup> Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), kakor je bila spremenjena z Direktivo 2009/136/ES z dne 25. novembra 2009 (UL L 337, str. 11).

<sup>4</sup> Členi 7, 8 in 52(1) Listine Evropske unije o temeljnih pravicah.

ureditev se mora opreti na **objektivna merila pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do podatkov**. Dostop je načeloma mogoče odobriti v povezavi z namenom boja proti kriminalu le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so tako ali drugače povezane s tem kaznivim dejanjem. Vendar bi bilo mogoče v posebnih okoliščinah, kakršne so te, v katerih dejanja terorizma ogrožajo bistvene interese nacionalne varnosti, obrambe ali javne varnosti, dostop do podatkov drugih oseb prav tako odobriti, kadar obstajajo objektivni elementi, na podlagi katerih je mogoče šteti, da bi ti podatki lahko v konkretnem primeru učinkovito prispevali k boju proti takim dejavnostim.

Dalje Sodišče meni, da **je bistveno, da za dostop do hranjenih podatkov – razen v nujnih primerih – predhodni nadzor** opravi sodišče ali neodvisen upravni organ. Poleg tega morajo pristojni nacionalni organi, ki jim je bil odobren dostop do hranjenih podatkov, o tem obvestiti zadevne osebe.

Glede na količino hranjenih podatkov, občutljivost teh podatkov in tveganje za nezakonit dostop do njih **mora nacionalna ureditev določiti, da se podatki hranijo na ozemlju Unije** in da se nepreklicno uničijo po koncu obdobja njihove hrambe.

---

**OBVESTILO:** S predlogom za sprejetje predhodne odločbe lahko sodišča držav članic v zvezi s sporom, o katerem odločajo, Sodišču predložijo vprašanja o razlagi prava Unije ali veljavnosti aktov Unije. Sodišče ne odloči o nacionalnem sporu. Zadevo reši nacionalno sodišče v skladu z odločbo Sodišča. Ta odločba je enako zavezujoča za druga nacionalna sodišča, ki obravnavajo podoben problem.

---

*Neuradni dokument za medije, ki Sodišča ne zavezuje.*

*[Celotno besedilo](#) sodbe je objavljeno na spletnem mestu CURIA na dan razglasitve.*

*Kontaktna oseba: Ireneusz Kolowca ☎ (+352) 4303 2793*

*Posnetki z razglasitve sodbe so dostopni na „[Europe by Satellite](#)“ ☎ (+32) 22964106*