Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
M. CAMPOSA SANCHEZ-BORDONE,
predstavljeni 15. januarja 2020 [1]

Zadeva C-623/17

Privacy International
proti
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service Srl,
Secret Intelligence Service

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo))

„Predhodno odločanje – Obdelava osebnih podatkov in varstvo zasebnega življenja na področju elektronskih komunikacij – Direktiva 2002/58 – Področje uporabe – Člen 1(3) – Člen 15(3) – Listina Evropske unije o temeljnih pravicah – Členi 7, 8, 51 in 52(1) – Člen 4(2) PEU – Splošen in neselektiven prenos podatkov o povezavi uporabnikov elektronske komunikacijske storitve varnostnim službam“

1. Sodišče je v zadnjih letih v zvezi s hrambo in dostopom do osebnih podatkov izoblikovalo ustaljeno sodno prakso, v okviru katere so bile prelomne zlasti te sodbe:

– sodba z dne 8. aprila 2014, Digital Rights Ireland in drugi [2], v kateri je razglasilo neveljavnost Direktive 2006/24/ES [3], ker je omogočala nesorazmeren poseg v pravice, priznane s členoma 7 in 8 Listine Evropske unije o temeljnih pravicah;

– sodba z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi [4], v kateri je razlagalo člen 15(1) Direktive 2002/58/ES [5];

– sodba z dne 2. oktobra 2018, Ministerio Fiscal [6], v kateri je potrdilo razlago te iste določbe iz Direktive 2002/58.

1 Jezik izvirnika: španščina.

2 Zadevi C-293/12 in C-594/12, v nadaljevanju: sodba Digital Rights, EU:C:2014:238.

3 Direktiva 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 2006, L 105, str. 54).

4 Zadevi C-203/15 in C-698/15, v nadaljevanju: sodba Tele2 Sverige in Watson, EU:C:2016:970.

5 Direktiva 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).

6 Zadeva C-207/16, v nadaljevanju: sodba Ministerio Fiscal, EU:C:2018:788.

2. Te sodbe (zlasti drugonavedena) organom nekaterih držav članic povzročajo skrbi, saj so po njihovem mnenju zaradi njih oropani instrumenta, ki ga štejejo za nujnega za zagotavljanje nacionalne varnosti in za boj proti terorizmu. Zato se nekatere od teh držav članic zavzemajo za preklic oziroma za prilagoditev te sodne prakse.

3. Nekatera sodišča držav članic so to zaskrbljenost izrazila v štirih predlogih za sprejetje predhodne odločbe[7], v zvezi s katerimi na isti dan predstavljam sklepne predloge.

4. Te štiri zadeve obravnavajo predvsem vprašanje uporabe Direktive 2002/58 za dejavnosti, ki so povezane z nacionalno varnostjo in bojem proti terorizmu. Če se ta direktiva v tem okviru uporabi, je nato treba razjasniti, v kolikšnem obsegu lahko države članice omejijo pravice do zasebnosti, ki so z njo varovane. Nazadnje je treba analizirati, v kolikšnem obsegu so različne nacionalne ureditve (britanska,[8] belgijska[9] in francoska[10]) tega področja skladne s pravom Unije, kakor ga je razlagalo Sodišče.

I. Pravni okvir

A. Pravo Unije

5. Napotujem na isto točko mojih sklepnih predlogov v zadevah C-511 in C-512/18.

B. Nacionalno pravo (ki velja za spor o glavni stvari)

1. Telecommunications Act 1984[11]

6. V skladu s členom 94 lahko Secretary of State upravljavcu javnega elektronskega komunikacijskega omrežja da taka splošna ali posebna navodila, za katera šteje, da so nujna v interesu nacionalne varnosti ali razmerjih z vlado države ali ozemlja zunaj Združenega kraljestva.

2. Data Retention and Investigatory Powers Act 2014[12]

7. Člen 1 določa:

„1. Secretary of State lahko z odločbo o hrambi od javnega telekomunikacijskega operaterja zahteva hrambo upoštevnih komunikacijskih podatkov, če meni, da je zahteva nujna in sorazmerna iz enega ali več razlogov, navedenih v točkah od (a) do (h) člena 22(2) Regulation of Investigatory Powers Act 2000 [(zakon o preiskovalnih pooblastilih iz leta 2000; v nadaljevanju: RIPA)].

2. Odločba o hrambi lahko:

(a) velja za določenega operaterja ali kakršne koli kategorije operaterjev,

(b) zahteva hrambo vseh podatkov ali kakršne koli kategorije podatkov,

7 Poleg te gre za zadevi C-511/18 in C-512/18, La Quadrature du Net in drugi, ter zadevo C-520/18, Ordre des barreaux francophones et germanophone in drugi.

8 Zadeva Privacy International, C-623/17.

9 Zadeva Ordre des barreaux francophones et germanophone in drugi, C-520/18.

10 Zadevi La Quadrature du Net in drugi, C-511/18 in C-512/18.

11 Zakon o telekomunikacijah iz leta 1984; v nadaljevanju: zakon iz leta 1984.

12 Zakon o hrambi podatkov in preiskovalnih pooblastilih iz leta 2014, v nadaljevanju: DRIPA.

(c) določi obdobje ali obdobja, ko je treba podatke hraniti,

(d) vsebuje druge zahteve ali omejitve v zvezi s hrambo podatkov,

(e) uvede različne določbe za različne namene,

(f) se nanaša na podatke, ki obstajajo ob izdaji ali začetku veljavnosti odločbe ali pa takrat še ne obstajajo.

3. Secretary of State lahko s pravilnikom sprejme dodatne določbe o hrambi upoštevnih komunikacijskih podatkov.

4. Te določbe se lahko zlasti nanašajo na:

(a) zahteve pred izdajo odločbe o hrambi,

(b) maksimalno obdobje, v katerem se podatki lahko hranijo na podlagi odločbe o hrambi,

(c) vsebino, izdajo, začetek veljavnosti, pregled, spremembo ali preklic odločbe o hrambi,

(d) celovitost, varnost ali varstvo hranjenih podatkov na podlagi tega člena, dostop do podatkov in njihovo razkritje ali uničenje,

(e) izvajanje upoštevnih zahtev ali omejitev oziroma preverjanje skladnosti s temi zahtevami ali omejitvami,

(f) kodeks ravnanja v zvezi z upoštevnimi zahtevami, omejitvami ali pooblastili,

(g) povračilo (pod pogoji ali brezpogojno) stroškov, ki nastanejo javnim telekomunikacijskim operaterjem zaradi upoštevanja upoštevnih zahtev ali omejitev, s strani Secretary of State,

[…]

5. Maksimalno obdobje, določeno na podlagi člena 4(b), ne sme preseči 12 mesecev od datuma, navedenega v zvezi s podatki, na katere se nanaša pravilnik iz tretjega odstavka.

6. Javni telekomunikacijski operater, ki hrani upoštevne komunikacijske podatke na podlagi tega člena, teh podatkov ne sme razkriti, razen če:

(a) jih razkrije v skladu s:

(i) poglavjem 2 dela 1 [RIPA] ali

(ii) sodno odločbo ali katerim koli drugim sodnim dovoljenjem ali nalogom ali če

(b) je tako določeno v pravilniku, na katerega se nanaša odstavek 3.

7. Secretary of State lahko s pravilniki sprejme določbe, ki ustrezajo kakršni koli sprejeti določbi (ali določbi, ki bi lahko bila sprejeta) v skladu z odstavkoma 4, od (d) do (g), ali 6 v zvezi s komunikacijskimi podatki, ki jih hranijo ponudniki telekomunikacijskih storitev na podlagi kodeksa ravnanja iz člena 102 Anti-terrorism, Crime and Security Act 2001 [(zakon o boju proti terorizmu, kriminalu in varnosti iz leta 2001)]“.

3. RIPA

8. Člen 21 določa:

„[…]

4. V tem poglavju ‚komunikacijski podatki' pomenijo kar koli od spodaj navedenega:

(a) vse podatke o prometu, ki so v sporočilu ali so sporočilu priloženi (s strani pošiljatelja ali kako drugače), za namene kakršne koli poštne storitve ali telekomunikacijskega sistema, s katerim se ali se lahko prenašajo;

(b) vsako informacijo, ki ne vključuje nobene vsebine sporočila (razen informacij, ki spadajo pod točko (a)) in ki se nanaša na uporabo s strani katere koli osebe:

(i) katere koli poštne ali telekomunikacijske storitve ali

(ii) v zvezi z zagotavljanjem katere koli telekomunikacijske storitve katerega koli dela telekomunikacijskega sistema kateri koli osebi ali z uporabo te storitve s strani katere koli osebe;

(c) vsako informacijo, ki ni zajeta s točkama (a) ali (b) ter ki jo ima ali jo pridobi oseba, ki zagotavlja poštno ali telekomunikacijsko storitev, v zvezi z osebami, za katere opravlja to storitev.

[…]

6. V tem členu se pojem ‚podatek o prometu' v zvezi s katero koli komunikacijo nanaša na:

(a) vsak podatek, s katerim se identificira ali se lahko identificira oseba, naprava ali lokacija, kamor ali od koder je ali je lahko komunikacija posredovana;

(b) vsak podatek, s katerim se identificira ali izbere oziroma se lahko identificira ali izbere naprava, prek katere ali s katero se oziroma se lahko komunikacija posreduje;

(c) vsak podatek, ki zajema signale za aktiviranje naprave, ki se uporablja v telekomunikacijskem sistemu za prenos komunikacij; in

(d) vsak podatek, ki identificira podatke ali druge podatke, zajete v konkretni komunikaciji oziroma priložene tej komunikaciji.

[…]"

9. Člen 22 določa:

„1. Ta člen se uporabi, če oseba, odgovorna v smislu tega poglavja, iz razlogov, naštetih v odstavku 2 tega člena, šteje, da je nujno pridobiti vse komunikacijske podatke.

2. Iz razlogov iz tega odstavka je nujno pridobiti komunikacijske podatke, če so potrebni

(a) v interesu nacionalne varnosti,

(b) za preprečevanje ali odkrivanje kriminala ali preprečevanje motenja javnega reda,

(c) v interesu gospodarske blaginje Združenega kraljestva, kadar so ti interesi pomembni tudi za interese nacionalne varnosti,

(d) v interesu javne varnosti,

(e) za varovanje javnega zdravja,

(f) za oceno naložitve ali izterjave davka, dajatve, pristojbine ali drugega bremena, prispevka ali obveznosti, ki se dolguje javni upravi,

(g) za preprečevanje – v nujnem primeru – smrti, poškodbe ali kakršne koli škode za telesno ali duševno zdravje osebe oziroma za ublažitev kakršne koli poškodbe ali škode za telesno ali duševno zdravje osebe,

(h) iz katerega koli razloga (ki ni zajet v točkah od (a) do (g)), opredeljenega v odločbi Secretary of State v skladu s členom 22(2)(h) [DRIPA].

4. Ob upoštevanju odstavka 5, če se odgovorni osebi zdi, da telekomunikacijski operater ali izvajalec poštnih storitev ima podatke, bi jih lahko imel oziroma bi jih lahko pridobil, lahko od telekomunikacijskega operaterja ali izvajalca poštnih storitev zahteva, da:

(a) pridobi podatke, če jih še nima, in

(b) v vsakem primeru razkrije vse podatke, ki jih ima ali ki jih je pridobil naknadno.

5. Odgovorna oseba ne izda dovoljenja v skladu z odstavkom 3 oziroma ne izda zahteve na podlagi odstavka 4, razen če meni, da pridobitev zadevnih podatkov, ki je posledica dovoljenega ali zahtevanega ravnanja na podlagi dovoljenja ali zahteve, sorazmerna s ciljem pridobitve podatkov.“

10. V skladu s členom 65 je treba zadevo predložiti Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo), če obstaja razlog za sum, da so bili podatki pridobljeni neprimerno.

II. Dejansko stanje in vprašanja za predhodno odločanje

11. Po navedbah predložitvenega sodišča se postopek v glavni stvari nanaša na pridobivanje in uporabo zbirnih komunikacijskih podatkov s strani United Kingdom Security and Intelligence Agencies (varnostno-obveščevalne agencije Združenega kraljestva, v nadaljevanju: VOA).

12. Ti podatki zajemajo podatke o tem, „kdo“ uporablja telefon in internet ter „kdaj, kje, kako in s kom“ ju uporablja. Zajemajo lokacijo mobilnih in stacionarnih telefonov, s katerih se kliče ali na katerih se klici sprejemajo, ter lokacijo računalnikov, ki se uporabljajo za dostop do interneta. Ne zajemajo pa vsebine komunikacij, ki se lahko pridobi samo z odredbo sodišča.

13. Tožeča stranka v postopku v glavni stvari (Privacy International, nevladna organizacija za varstvo človekovih pravic) je pri predložitvenem sodišču vložila tožbo, v kateri trdi, da sta pridobivanje in uporaba omenjenih podatkov s strani VOA kršitev pravice do zasebnega življenja iz člena 8 Evropske konvencije o človekovih pravicah (v nadaljevanju: EKČP) in v nasprotju s pravom Unije.

14. Toženi organi[13] trdijo, da je uporaba njihovih pooblastil zakonita in bistvena, med drugim, za varovanje nacionalne varnosti.

15. Glede na informacije v predložitveni odločbi VOA na podlagi navodil, ki jih je izdal Secretary of State v skladu s členom 94 zakona iz leta 1984, prejemajo zbirne komunikacijske podatke od operaterjev javnih elektronskih komunikacijskih omrežij.

16. Navedeni podatki zajemajo podatke o prometu in lokaciji ter o družbenih, poslovnih in finančnih dejavnostih, komunikacijah in potovanjih uporabnikov. VOA te podatke, ko jih imajo v posesti, varno hranijo, tako da uporabijo splošne tehnike (na primer filtriranje in združevanje), to pomeni, da niso usmerjene na konkretne in znane cilje.

17. Predložitveno sodišče glede na predložene dokaze meni, da so te tehnike bistvene za delo VOA pri boju proti resnim grožnjam javni varnosti, zlasti terorizmu, vohunjenju in širjenju jedrskega orožja. Zmožnosti pridobivanja in uporabe podatkov s strani VOA so bistvene za varovanje nacionalne varnosti Združenega kraljestva.

18. Po mnenju predložitvenega sodišča so sporni ukrepi v skladu z nacionalnim pravom in členom 8 EKČP. Vendar navedeno sodišče glede na sodbo Tele2 Sverige in Watson dvomi o njihovi združljivosti s pravom Unije.

19. V teh okoliščinah je navedeno sodišče Sodišču predložilo ta vprašanja za predhodno odločanje:

„1. Ali ob upoštevanju člena 4 PEU in člena 1(3) Direktive 2002/58[…] zahteva v navodilu Secretary of State, da mora ponudnik elektronskega komunikacijskega omrežja varnostno-obveščevalnim agencijam ([VOA]) države članice posredovati zbirne komunikacijske podatke, spada na področje uporabe prava Unije in Direktive [2002/58]?

2. Če je odgovor na prvo vprašanje pritrdilen, ali se za tako navodilo Secretary of State uporabljajo katere od zahtev iz sodbe Watson[14] ali katere druge zahteve poleg tistih iz EKČP? In če se, kako in v kakšnem obsegu se take zahteve uporabljajo ob upoštevanju bistvene potrebe VOA, da uporabljajo tehnike zbirnega pridobivanja in samodejne obdelave za varovanje nacionalne varnosti, in obsega, v katerem so lahko take zmožnosti, če so sicer skladne z EKČP, bistveno ogrožene z naložitvijo takih zahtev?“

20. Predložitveno sodišče umešča svoja vprašanja v ta okvir:

„(a) zmožnost [VOA], da uporabljajo posredovane jim [zbirne komunikacijske podatke], je bistvena za varovanje nacionalne varnosti Združenega kraljestva, vključno na področju boja proti terorizmu, protiobveščevalni dejavnosti in širjenju jedrskega orožja;

(b) temeljna značilnost uporabe [teh podatkov] s strani VOA je odkrivanje prej neznanih groženj nacionalni varnosti s tehnikami neusmerjenega zbiranja, ki temeljijo na zbiranju [teh podatkov] na enem mestu. Glavna uporabnost tega je hitro identificiranje in razvoj ciljev ter zagotavljanje podlage za ukrepanje ob neposrednih grožnjah;

(c) od ponudnika elektronskega komunikacijskega omrežja se nato ne zahteva hramba omenjenih podatkov (za dalj časa kot pri običajnem poslovanju), ki jih hrani izključno država (VOA);

13 Secretary of State for Foreign and Commonwealth Affairs (minister za zunanje zadeve in Commonwealth), Secretary of State for the Home Department (minister za notranje zadeve) ter tri VOA Združenega kraljestva, in sicer Government Communications Headquarters (vlada uprava za komunikacije, GCHQ), Security Service (varnostna služba, MI5) in Secret Intelligence Service (tajna obveščevalna služba, MI6).

14 Tj. sodna praksa iz sodbe Tele2 Sverige in Watson.

(d) nacionalno sodišče (z nekaterimi pridržanimi vprašanji) je presodilo, da so jamstva v zvezi z uporabo [teh podatkov] s strani VOA skladna z zahtevami EKČP; in

(e) nacionalno sodišče je presodilo, da bi se z naložitvijo zahtev iz sodbe [Tele2 Sverige ter Watson], če bi jih bilo mogoče uporabiti, ogrozili ukrepi VOA za varovanje nacionalne varnosti, s tem pa bi se ogrozila nacionalna varnost Združenega kraljestva."

III. Postopek pred Sodiščem

21. Predlog za sprejetje predhodne odločbe je bil v sodnem tajništvu Sodišča vpisan 31. oktobra 2017.

22. Nemška, belgijska, britanska, češka, ciprska, španska, estonska, francoska, madžarska, irska, latvijska, nizozemska, norveška, poljska, portugalska in švedska vlada ter Komisija so predložile pisna stališča.

23. Obravnava je bila 9. septembra 2019 in se je opravila skupaj z obravnavama v zadevah C-511/18, C-512/18 in C-520/18, udeležile pa so se je stranke iz štirih postopkov za sprejetje predhodne odločbe, zgoraj navedene vlade ter Komisija in Evropski nadzornik za varstvo podatkov.

IV. Analiza

A. Področje uporabe Direktive 2002/58 in izključitev nacionalne varnosti (prvo vprašanje za predhodno odločanje)

24. V sklepnih predlogih, ki jih na isti datum predstavljam v zadevah C-511/18 in C-512/18, pojasnjujem razloge, zaradi katerih se po mojem mnenju Direktiva 2002/58 „načeloma uporabi, kadar ponudnike elektronskih storitev zakon zavezuje, da hranijo podatke svojih naročnikov in da javnim organom omogočijo, da do njih dostopijo. To, da se obveznosti ponudnikom naložijo iz razlogov nacionalne varnosti, ne spremeni te trditve." [15]

25. Pri izpeljavi svojih argumentov obravnavam vpliv sodb Sodišča z dne 30. maja 2006, Parlament/Svet in Komisija [16], ter Tele2 Sverige in Watson, pri tem pa zagovarjam usklajeno razlago obeh. [17]

26. V teh istih sklepnih predlogih najprej potrdim uporabo Direktive 2002/58, nato pa preučim izključitev nacionalne varnosti, ki je tam navedena, in vpliv člena 4(2) PEU. [18]

27. Ne da bi to vplivalo na to, kar pojasnjujem spodaj, napotujem na to, kar sem že povedal v navedenih sklepnih predlogih in v sklepnih predlogih v zadevi C-520/18.

15 Sklepni predlogi v zadevah C-511/18 in C-512/18, točka 42.

16 Zadevi C-317/04 in C-318/04, EU:C:2006:346.

17 Sklepni predlogi v zadevah C-511/18 in C-512/18, točke od 44 do 76.

18 Prav tam, točke od 77 do 90.

1. Uporaba Direktive 2002/58 v tej zadevi

28. V skladu s predpisi, ki so sporni v tem postopku, so ponudniki elektronskih komunikacijskih storitev naslovniki obveznosti, ki poleg hrambe podatkov zajema tudi obdelavo podatkov, ki jih imajo zaradi storitve, ki jo opravljajo za uporabnike javnih komunikacijskih omrežij Unije. [19]

29. Omenjeni operaterji morajo namreč te podatke obvezno poslati VOA. Vprašanje, ki se tu zastavi, je, ali člen 15(1) Direktive 2002/58 dopušča, da se ta prenos glede na njegov cilj kar tako izključi iz prava Unije.

30. Po mojem mnenju ni tako. Hrambo navedenih podatkov, ki ji sledi naknaden prenos, je mogoče opredeliti kot obdelavo osebnih podatkov s strani ponudnikov elektronskih komunikacijskih storitev, zaradi česar seveda spadajo na področje uporabe Direktive 2002/58.

31. Razlogi nacionalne varnosti ne morejo imeti prednosti pred to ugotovitvijo, kot predlaga predložitveno sodišče, zaradi česar sporna obveznost ne bi spadala na področje uporabe prava Unije. Če ponovim, menim, da se ponudnikom nalaga obdelava podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji, kar je v skladu s členom 3(1) Direktive 2002/58 ravno njeno področje.

32. Glede na to se razprava ne nanaša več na dejavnosti VOA (ki bi lahko bile, kot sem prej opozoril, zunaj prava Unije, če ne bi vplivale na operaterje elektronskih komunikacij), temveč se preusmeri na hrambo in naknaden prenos podatkov, ki so v rokah teh operaterjev. S tega vidika pa v igro vstopijo temeljne pravice, ki jih zagotavlja Unija.

33. Ključni dejavnik za odločitev v tej razpravi je ponovno dolžnost splošne in neselektivne hrambe podatkov, do katerih lahko dostopajo javni organi.

2. Sklicevanje na nacionalno varnost

34. Ker predložitveno sodišče v tej zadevi posebej poudarja dejavnost VOA, ki se nanaša na nacionalno varnost, naj tu citiram nekatere točke mojih sklepnih predlogov z istega dne v združenih zadevah C-511/18 in C-512/18 glede tega primera:

„77. Nacionalna varnost […] je v tej direktivi upoštevana z dveh vidikov. Po eni strani je razlog za izključitev (iz področja uporabe te direktive) vseh teh dejavnosti držav članic, ki so konkretno z njo ‚v zvezi'. Po drugi strani pa pomeni razlog za omejitev – ki mora biti opredeljena z zakonom – pravic in obveznosti, določenih z Direktivo 2002/58, torej teh, ki se nanašajo na zasebne ali poslovne dejavnosti, ki niso povezane z oblastnimi dejavnostmi.

78. Na katere dejavnosti se nanaša člen 1(3) Direktive 2002/58? Menim, da je sam Conseil d'État (državni svet) podal dober primer s tem, da je omenil določbe členov L. 851-5 in L. 851-6 zakonika o notranji varnosti, pri čemer se je skliceval na ‚metode pridobivanja informacij, ki jih neposredno izvaja država, ne da bi urejale dejavnosti ponudnikov elektronskih komunikacijskih storitev in jim nalagale posebne obveznosti'. […]

19 V skladu s členom 2 Direktive 2002/58 se za namene te direktive uporabijo opredelitve pojmov iz Direktive 95/46. V skladu s členom 2(b), te direktive „obdelava osebnih podatkov" „pomeni kakršen koli postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki z avtomatskimi sredstvi ali brez njih, kakršno je zbiranje, beleženje, urejanje, shranjevanje, prilagajanje ali predelava, iskanje, posvetovanje, uporaba, *posredovanje s prenosom*, širjenje ali *drugo razpolaganje*, prilagajanje ali kombiniranje, blokiranje, izbris ali uničenje" (moj poudarek).

79. Menim, da je v tem ključ za določitev obsega izključitve iz člena 1(3) Direktive 2002/58. Ureditev iz te direktive se ne uporablja za dejavnosti, ki so namenjene zaščiti nacionalne varnosti in jih javne oblasti izvajajo v svojem imenu, ne da bi pri tem zahtevale sodelovanje zasebnikov, ki jim torej ne naložijo obveznosti pri poslovnem upravljanju.

80. Vendar je treba seznam dejavnosti javnih oblasti, ki so izvzete iz splošne ureditve o obdelavi osebnih podatkov, razlagati ozko. Konkretno, pojma *nacionalne varnosti*, ki je v skladu s členom 4(2) PEU v izključni pristojnosti vsake države članice, ni mogoče razširiti na druge, bolj ali manj sorodne sektorje javnega življenja.

[…]

82. [M]enim, da bi bilo kot smernica v zvezi s tem lahko koristno merilo iz Okvirnega sklepa 2006/960/PNZ[…], v členu 2(a) katerega se razlikuje med organi kazenskega pregona v širšem pomenu – ki vključujejo ‚državno policijo, carino ali drug organ, ki mu nacionalna zakonodaja daje pooblastila za odkrivanje, preprečevanje in preiskovanje kaznivih dejanj ali kriminalnih dejavnosti ter za izvajanje pooblastil in uporabo prisilnih ukrepov v okviru takšnih dejavnosti' – na eni strani ter ‚[a]gencij[ami] ali enot[ami], ki se ukvarjajo posebej z vprašanji državne varnosti', na drugi. […]

[…]

84. Glede pristojnosti držav članic v zvezi z nacionalno varnostjo je med Direktivo 95/46 in Direktivo 2002/58 […] kontinuiteta. Nobena se ne nanaša na varstvo temeljnih pravic na tem konkretnem področju, na katerem dejavnosti držav članic ‚ne ureja pravni red [Unije]'.

85. ‚Ravnotežje', omenjeno v […] uvodni izjavi [11 Direktive 2002/58], izhaja iz zahteve po spoštovanju pristojnosti držav članic na področju nacionalne varnosti, kadar jih te izvajajo *neposredno* in *z lastnimi sredstvi*. Okoliščina, da se – pa čeprav zaradi razlogov nacionalne varnosti – zahteva sodelovanje zasebnikov, ki se jim naložijo določene obveznosti, je podlaga za uvrstitev na področje (varstvo zasebnosti, ki ga morajo spoštovati ti zasebni subjekti), ki je urejeno s pravom Unije.

86. V direktivah 95/46 in 2002/58 se skuša to ravnotežje doseči z določitvijo, da se lahko pravice zasebnikov omejijo na podlagi zakonskih ukrepov, ki jih države sprejmejo na podlagi členov 13(1) oziroma 15(1) omenjenih direktiv. Glede tega med njima ni nobenih razlik.

[…]

89. Opredelitev teh dejavnosti, ki jih opravlja javna oblast, mora biti ozka, saj se sicer okrni polni učinek prava Unije na področju varstva zasebnosti. V členu 23 Uredbe 2016/679 je – podobno kot v členu 15(1) Direktive 2002/58 – določena možnost, da se *z zakonodajnimi ukrepi* omejijo pravice in obveznosti, ki jih ta uredba določa, če je to potrebno za zagotavljanje, med drugim, državne varnosti, obrambe ali javne varnosti. In spet: če bi varstvo teh ciljev zadostovalo za izključitev iz področja uporabe Uredbe 2016/679, potem bi bila odveč določitev, da je na podlagi državne varnosti mogoče upravičiti to, da se z zakonodajnimi ukrepi omejijo pravice, zagotovljene s to uredbo."

3. Posledice uporabe sodbe Tele2 Sverige in Watson za to zadevo

35. Predložitveno sodišče se je osredotočilo na razlago, ki jo je Sodišče podalo v sodbi Tele2 Sverige in Watson, pri čemer je izpostavilo težave, ki bi jih po njegovem mnenju povzročila uporaba te sodbe za to zadevo.

36. V sodbi Tele2 Sverige in Watson so namreč navedeni pogoji, ki jih mora izpolniti nacionalna ureditev, ki uvaja obveznost hrambe podatkov o prometu in lokaciji, da bi nato do njih lahko dostopali javni organi.

37. Tako kot v združenih zadevah C-511/18 in C-512/18 ter iz podobnih razlogov menim, da nacionalni predpisi, na katere se nanaša ta predlog za sprejetje predhodne odločbe, ne upoštevajo pogojev, določenih v sodbi Tele2 Sverige in Watson, saj pomenijo splošno in neselektivno hrambo osebnih podatkov, ki zagotavlja podrobno poročilo o življenju prizadetih oseb v daljšem obdobju.

38. V sklepnih predlogih v navedenih dveh zadevah sem se spraševal, ali bi bilo mogoče podrobneje opredeliti ali dopolniti sodno prakso, opisano v navedeni sodbi, glede na njene posledice za boj proti terorizmu ali za varstvo države pred drugimi podobnimi grožnjami nacionalni varnosti.

39. Tudi v tem primeru bom v nadaljevanju citiral nekatere točke omenjenih sklepnih predlogov, v katerih v bistvu trdim, da je treba navedeno sodno prakso, ker jo je mogoče nekoliko prilagoditi, v bistvenem potrditi:

„135. Natančna in na podlagi objektivnih meril opravljena opredelitev kategorij podatkov, katerih hramba se šteje za nujno, in kroga zadevnih oseb je zahtevna, ne pa tudi nemogoča. Seveda bi bila najbolj praktična in učinkovita splošna hramba vseh podatkov, ki jih lahko zberejo ponudniki elektronskih komunikacijskih storitev, vendar […] se vprašanje ne more reševati ob upoštevanju *praktične učinkovitosti*, temveč ob upoštevanju *pravne učinkovitosti* in v okviru pravne države.

136. Ta opredelitev se tipično opravi v okviru zakonodaje, izvesti pa se mora ob upoštevanju omejitev iz sodne prakse Sodišča. […]

137. Ob predpostavki, da so operaterji podatke zbrali ob spoštovanju določb Direktive 2002/58 in da je bila njihova hramba izvedena ob upoštevanju člena 15(1) […] te direktive, lahko pristojni organi do teh podatkov dostopajo pod pogoji, ki morajo biti izpolnjeni v skladu s sodno prakso Sodišča in ki sem jih analiziral v sklepnih predlogih v zadevi C-520/18, na katere napotujem.

138. Zato je treba tudi v tem primeru z nacionalno ureditvijo določiti vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov. […] V okviru tega postopka za sprejetje predhodne odločbe bi bil v skladu s temi pogoji dovoljen dostop do podatkov oseb, ki so osumljene, da načrtujejo ali da bodo storile teroristično dejanje, ali ki so storile ali ki bi bile lahko vpletene v teroristično dejanje. […]

139. Vendar je bistveno to, da za dostop do zadevnih podatkov, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi predhoden nadzor in da se odločba tega sodišča ali tega organa izda na obrazloženi predlog pristojnih organov. […] Tako je v primerih, ki se ne morejo rešiti s presojo *in abstracto* na podlagi zakona, zagotovljena presoja *in concreto* tega neodvisnega organa, ki je enako zavezan zagotavljanju državne varnosti in varovanju temeljnih pravic državljanov“.

B. Drugo vprašanje za predhodno odločanje

40. Predložitveno sodišče svoje drugo vprašanje postavlja samo, če bi bil odgovor na prvo pritrdilen. V takem primeru želi vedeti, katere „druge zahteve poleg tistih iz EKČP“ ali tistih, ki izhajajo iz sodbe Tele2 Sverige in Watson, bi bilo treba določiti.

41. V tem smislu trdi, da bi se z naložitvijo zahtev iz sodbe Tele2 Sverige ter Watson „ogrozili ukrepi VOA za varovanje nacionalne varnosti“.

42. Ker je odgovor, ki ga predlagam na prvo vprašanje, nikalen, ni treba obravnavati drugega. To zadnje vprašanje je, kot je poudarilo samo predložitveno sodišče, pogojeno s tem, da se „tehnike zbirnega pridobivanja in samodejne obdelave“ osebnih podatkov vseh uporabnikov v Združenem kraljestvu, ki bi jih ponudniki elektronskih komunikacijskih storitev morali posredovati VOA, razglasijo za skladne s pravom Unije.

43. Če bi Sodišče ocenilo, da je na drugo vprašanje treba odgovoriti, menim, da bi moralo potrditi navedene pogoje iz sodbe Tele2 Sverige in Watson v zvezi s:

– prepovedjo splošnega dostopa do podatkov;

– z nujnim predhodnim dovoljenjem sodnika ali neodvisnega organa, s katerim se ta dostop upraviči;

– z obveznostjo obveščanja prizadetih oseb, razen če bi se s tem ogrozila učinkovitost ukrepa;

– s hrambo podatkov v Uniji.

44. Ponavljam, da bi zadostovala potrditev teh pogojev, katerih uporaba je obvezna, iz razlogov, ki sem jih pojasnil v sklepnih predlogih v zadevah C-511/18 in C-512/18 ter C-520/18, ne da bi bilo treba uvajati „druge“ dodatne pogoje, kot navaja predložitveno sodišče.

V. Predlog

45. Na podlagi zgornjih ugotovitev Sodišču predlagam, naj Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo) odgovori tako:

Člen 4 PEU in člen 1(3) Direktive 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) je treba razlagati tako, da nasprotujeta nacionalni ureditvi, ki ponudniku elektronskih komunikacijskih omrežij nalaga obveznost, da varnostnim in obveščevalnim agencijam države članice posreduje „zbirne komunikacijske podatke“, kar pomeni, da so bili prej splošno in neselektivno zbrani.

Podredno:

Dostop do podatkov, ki jih posredujejo ponudniki elektronskih komunikacijskih omrežij, s strani varnostnih in obveščevalnih agencij države članice mora biti v skladu s pogoji, določenimi v sodbi z dne 21. decembra 2016, Tele2 Sverige in Watson (C-203/15 in C-698/15, EU:C:2016:970).