



Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 6. oktobra 2020*

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Ponudniki elektronskih komunikacijskih storitev – Splošno in neselektivno posredovanje podatkov o prometu in podatkov o lokaciji – Zaščita nacionalne varnosti – Direktiva 2002/58/ES – Področje uporabe – Člen 1(3) in člen 3 – Zaupnost elektronskih komunikacij – Varstvo – Člen 5 in člen 15(1) – Listina Evropske unije o temeljnih pravicah – Členi 7, 8 in 11 ter člen 52(1) – Člen 4(2) PEU“

V zadevi C-623/17,

katere predmet je predlog za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki ga je vložilo Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo) z odločbo z dne 18. oktobra 2017, ki je na Sodišče prispela 31. oktobra 2017, v postopku

Privacy International

proti

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

SODIŠČE (veliki senat)

v sestavi K. Lenaerts, predsednik, R. Silva de Lapuerta, podpredsednica, J.-C. Bonichot, A. Arabadjiev, predsednika senatov, A. Prechal, predsednica senata, M. Safjan, P. G. Xuereb, predsednika senatov, in L. S. Rossi, predsednica senata, J. Malenovský, L. Bay Larsen, T. von Danwitz (poročevalec), sodniki, C. Toader, K. Jürimäe, sodnici, C. Lycourgos in N. Piçarra, sodnika,

generalni pravobranilec: M. Campos Sánchez-Bordona,

sodna tajnica: C. Strömholm, administratorka,

na podlagi pisnega postopka in obravnave z dne 9. in 10. septembra 2019,

* Jezik postopka: angleščina.

ob upoštevanju stališč, ki so jih predložili:

- za Privacy International B. Jaffey in T. de la Mare, QC, D. Cashman, solicitor, in H. Roy, avocat,
- za vlado Združenega kraljestva Z. Lavery, D. Guðmundsdóttir in S. Brandon, agenti, skupaj z G. Facenno in D. Beardom, QC, ter C. Knightom in R. Palmerjem, barristers,
- za belgijsko vlado P. Cottin in J.-C. Halleux, agenta, skupaj z J. Vanpraetom, advocaat, in E. de Lophemom, avocat,
- za češko vlado M. Smolek, J. Vlácil in O. Serdula, agenti,
- za nemško vlado sprva M. Hellmann, R. Kanitz, D. Klebs in T. Henze, nato J. Möller, M. Hellmann, R. Kanitz in D. Klebs, agenti,
- za estonsko vlado A. Kalbus, agentka,
- za irsko vlado M. Browne, G. Hodge in A. Joyce, agenti, skupaj z D. Fennellyjem, barrister,
- za špansko vlado sprva L. Aguilera Ruiz in M. J. García-Valdecasas Dorrego, nato L. Aguilera Ruiz, agenta,
- za francosko vlado sprva E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas in D. Dubois, nato E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune in D. Dubois, agenti,
- za ciprsko vlado E. Symeonidou in E. Neofytou, agentki,
- za latvijsko vlado sprva V. Soņeca in I. Kucina, nato V. Soņeca, agentki,
- za madžarsko vlado sprva G. Koós, M. Z. Fehér, G. Tornyai in Z. Wagner, nato G. Koós in M. Z. Fehér, agenti,
- za nizozemsko vlado C. S. Schillemans in M. K. Bulterman, agentki,
- za poljsko vlado B. Majczyna, J. Sawicka in M. Pawlicka, agenti,
- za portugalsko vlado L. Inez Fernandes, M. Figueiredo in F. Aragão Homem, agenti,
- za švedsko vlado sprva A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren in A. Alriksson, nato H. Shev, C. Meyer-Seitz, L. Zettergren in A. Alriksson, agentke,
- za norveško vlado T. B. Leming, M. Emberland in J. Vangsnes, agenti,
- za Evropsko komisijo sprva H. Kranenborg, M. Wasmeier, D. Nardi in P. Costa de Oliveira, nato H. Kranenborg, M. Wasmeier in D. Nardi, agenti,
- za Evropskega nadzornika za varstvo podatkov T. Zerdick in A. Buchta, agenta,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 15. januarja 2020

izreka naslednjo

Sodbo

- 1 Predlog za sprejetje predhodne odločbe se nanaša na razlago člena 1(3) in člena 15(1) 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) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11) (v nadaljevanju: Direktiva 2002/58), v povezavi s členom 4(2) PEU ter členi 7, 8 in 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).
- 2 Ta predlog je bil vložen v okviru spora med organizacijo Privacy International ter Secretary of State for Foreign and Commonwealth Affairs (minister za zunanje zadeve in Commonwealth, Združeno kraljestvo), Secretary of State for the Home Department (minister za notranje zadeve, Združeno kraljestvo), Government Communications Headquarters (vladna uprava za komunikacije, Združeno kraljestvo, v nadaljevanju: GCHQ), Security Service (varnostna agencija, Združeno kraljestvo, v nadaljevanju: MI5) in Secret Intelligence Service (tajna obveščevalna agencija, Združeno kraljestvo, v nadaljevanju: MI6) glede zakonitosti zakonodaje, ki varnostnim in obveščevalnim agencijam dovoljuje pridobivanje in uporabo masovnih komunikacijskih podatkov (*bulk communications data*).

Pravni okvir

Pravo Unije

Direktiva 95/46

- 3 Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355) je bila z učinkom od 25. maja 2018 razveljavljena z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (UL 2016, L 119, str. 1). Člen 3 navedene direktive, naslovljen „Področje uporabe“, je določal:

„1. Ta direktiva se uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatskimi sredstvi in za drugačno obdelavo kakor z avtomatskimi sredstvi za osebne podatke, ki sestavljajo del zbirke ali so namenjeni sestavljanju dela zbirke.

2. Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

- med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI [PEU], in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,
- s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti.“

Direktiva 2002/58

4 V uvodnih izjavah 2, 6, 7, 11, 22, 26 in 30 Direktive 2002/58 je navedeno:

„(2) Ta direktiva uveljavlja spoštovanje temeljnih pravic in upošteva načela, priznana zlasti z [Listino]. Zlasti pa želi ta direktiva zagotoviti popolno spoštovanje pravic, določenih v členih 7 in 8 navedene listine.

[...]

(6) Internet spreminja tradicionalne tržne strukture, ker ponuja skupno, globalno infrastrukturo za dobavo široke izbire elektronskih komunikacijskih storitev. Javno dostopne elektronske komunikacijske storitve prek interneta odpirajo nove možnosti uporabnikom, pa tudi nova tveganja za njihove osebne podatke in zasebnost.

(7) V primeru javnih komunikacijskih omrežij je treba sprejeti posebne zakone in druge predpise, s katerimi se zavarujejo temeljne pravice in svoboščine fizičnih oseb ter zakoniti interesi pravnih oseb, zlasti v zvezi s čedalje večjo zmogljivostjo samodejnega shranjevanja in obdelave podatkov, ki se nanašajo na naročnike in uporabnike.

[...]

(11) Ta direktiva, tako kot Direktiva [95/46], ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red [Unije]. Zato ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito javne varnosti, obrambe, državne varnosti (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve državne varnosti) in izvajanje kazenske zakonodaje. Ta direktiva torej ne vpliva na zmožnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so potrebni iz katerega koli od teh namenov ter v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin [podpisano v Rimu 4. novembra 1950], kakor jo razlaga Evropsko sodišče za človekove pravice v svojih sodbah. Taki ukrepi morajo biti ustrezni, dosledno sorazmerni z namenom in potrebni v demokratični družbi ter predmet primernih zaščitnih ukrepov v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.

[...]

(22) Prepoved shranjevanja sporočil in s tem povezanih podatkov o prometu osebam, ki niso uporabniki ali ki nimajo privolitve uporabnikov, ni namenjena prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa v omrežju elektronskih komunikacij in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena v času njihovega hranjenja. Kadar je to potrebno zaradi učinkovitejšega prenosa katerih koli javno dostopnih podatkov drugim prejemnikom storitve na njihovo zahtevo, ta direktiva ne preprečuje nadaljnjega hranjenja takih podatkov, pod pogojem da so ti podatki v vsakem primeru dostopni javnosti brez omejitev in da se vsi podatki, ki se nanašajo na posamezne naročnike ali uporabnike, ki zahtevajo take podatke, izbrišejo.

[...]

(26) Podatki o naročnikih, ki se obdelajo v elektronskih komunikacijskih omrežjih zaradi vzpostavitve povezav in prenosa podatkov, vsebujejo podatke o zasebnem življenju fizičnih oseb in zadevajo pravico do spoštovanja njihove korespondence ali legitimne interese pravnih oseb. Takšni

podatki se lahko shranijo le v obsegu, potrebnem za izvedbo storitve, za namen zaračunavanja in plačila medsebojnih povezav ter za določen čas. Vsaka nadaljnja obdelava takih podatkov [...] je dovoljena samo takrat, kadar naročnik v to privoli na podlagi točnih in popolnih podatkov, ki jih dobi od ponudnika javno razpoložljivih elektronskih komunikacijskih storitev o vrsti nadaljnje obdelave, ki jo ta namerava izvajati, in o naročnikovi pravici, da ne da privolitve za tako obdelavo ali da jo umakne. Podatke o prometu, uporabljene za trženje komunikacijskih storitev [...], je [...] treba izbrisati ali napraviti anonimne.

[...]

(30) Sistemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev morajo biti zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum. [...]"

5 Člen 1 Direktive 2002/58, naslovljen „Področje in cilj“, določa:

„1. Ta direktiva določa uskladitev [harmonizacijo] določb držav članic, ki je potrebna za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v [Evropski uniji].

2. Določbe te direktive podrobno opredeljujejo in dopolnjujejo Direktivo [95/46] za namene, navedene v odstavku 1. Razen tega predvidevajo varstvo zakonitih interesov naročnikov, ki so pravne osebe.

3. Ta direktiva se ne uporablja za dejavnosti, ki so zunaj obsega [PDEU], kot na primer tiste, zajete v Oddelkih V in VI Pogodbe o Evropski uniji in v vsakem primeru za dejavnosti v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo) ter dejavnosti države na področju kazenskega prava.“

6 Člen 2 te direktive, naslovljen „Opredelitve“, določa:

„Razen če je drugače določeno, se uporabijo opredelitve pojmov iz Direktive [95/46] in Direktive 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (Okvirna direktiva) [(UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 349)].

Uporabijo se tudi naslednje opredelitve pojmov:

- (a) ‚uporabnik‘ pomeni vsako fizično osebo, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev;
- (b) ‚podatki o prometu‘ pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila;
- (c) ‚podatki o lokaciji‘ pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve;
- (d) ‚sporočilo‘ (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve. To ne vključuje nobenih podatkov, prenesenih javnosti kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da podatek povezati s prepoznavnim naročnikom ali uporabnikom, ki ga prejme;

[...]“

7 Člen 3 navedene direktive, naslovljen „Storitve“, določa:

„Ta direktiva se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v [Uniji], vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave.“

8 Člen 5 Direktive 2002/58, naslovljen „Zaupnost sporočil“, določa:

„1. Države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Zlasti prepovejo vsem osebam razen uporabnikom, da poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1). Ta odstavek ne preprečuje tehničnega shranjevanja, ki je potrebno za prenos sporočila, brez vpliva na načelo zaupnosti.

[...]

3. Države članice zagotovijo, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo [95/46], med drugim o namenih obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.“

9 Člen 6 Direktive 2002/58, naslovljen „Podatki o prometu“, določa:

„1. Podatki o prometu, ki se nanašajo na naročnike in uporabnike in ki jih je ponudnik javnega komunikacijskega omrežja ali javno razpoložljive elektronske komunikacijske storitve obdelal in shranil, morajo biti izbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila, kar ne vpliva na odstavke 2, 3 in 5 tega člena in člena 15(1).

2. Podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave, se lahko obdelujejo. Taka obdelava je dovoljena samo do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila.

3. Za namen trženja elektronskih komunikacijskih storitev ali zagotovitve storitev z dodano vrednostjo lahko ponudnik javno razpoložljive elektronske komunikacijske storitve obdelata podatke iz odstavka 1 v obsegu in trajanju, ki sta potrebna za takšne storitve ali trženje, če naročnik ali uporabnik, na katerega se podatki nanašajo, v to prej privoli. Uporabnikom ali naročnikom je dana možnost, da kadar koli umaknejo privolitev v obdelavo podatkov o prometu.

[...]

5. Obdelava podatkov o prometu mora biti v skladu z odstavki 1, 2, 3 in 4 omejena na osebe, ki delujejo pod nadzorom ponudnikov javnih komunikacijskih omrežij in javno razpoložljivih elektronskih komunikacijskih storitev in ki skrbijo za zaračunavanje ali upravljanje prometa, se odzivajo na povpraševanje porabnikov, odkrivajo prevare, tržijo elektronske komunikacijske storitve ali zagotavljajo storitve z dodano vrednostjo, pri čemer mora biti ta obdelava omejena na to, kar je potrebno za namene takšnih dejavnosti.“

- 10 Člen 9 te direktive, naslovljen „Podatki o lokaciji razen podatkov o prometu“, v odstavku 1 določa:

„Kadar se podatki o lokaciji, razen podatkov o prometu, ki se nanašajo na uporabnike ali naročnike javnih komunikacijskih omrežij ali javno razpoložljivih elektronskih komunikacijskih storitev, dajo obdelovati, se smejo takšni podatki obdelati šele potem, ko postanejo anonimni ali s privolitvijo uporabnikov ali naročnikov in to v obsegu in trajanju, ki sta potrebna za izvedbo storitve z dodano vrednostjo. Ponudnik storitve mora pred pridobitvijo njihove privolitve obvestiti uporabnike ali naročnike o vrsti podatkov v zvezi z lokacijo, razen podatkov o prometu, ki bodo obdelani, o namenih in trajanju obdelave in ali bodo podatki poslani tretji osebi za namen izvedbe storitve z dodano vrednostjo. [...]“

- 11 Člen 15 navedene direktive, naslovljen „Uporaba nekaterih določb Direktive [95/46]“, v odstavku 1 določa:

„Države članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne [nacionalne] varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje Skupnosti, vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji.“

Uredba št. 2016/679

- 12 Člen 2 Uredbe št. 2016/679 določa:

„1. Ta uredba se uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatiziranimi sredstvi in za drugačno obdelavo kakor z avtomatiziranimi sredstvi za osebne podatke, ki so del zbirke ali so namenjeni oblikovanju dela zbirke.

2. Ta uredba se ne uporablja za obdelavo osebnih podatkov:

- (a) v okviru dejavnosti zunaj področja uporabe prava Unije;
- (b) s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 2 naslova V PEU;

[...]

- (d) s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.

[...]“

- 13 Člen 4 te uredbe določa:

„V tej uredbi:

[...]

- (2) ‚obdelava‘ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

[...]“

14 Člen 23(1) te uredbe določa:

„Pravo Unije ali pravo države članice, ki velja za upravljavca ali obdelovalca podatkov, lahko z zakonodajnim ukrepom omeji obseg obveznosti in pravic iz členov 12 do 22 in člena 34, pa tudi člena 5, kolikor njegove določbe ustrezajo pravicam in obveznostim iz členov 12 do 22, če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje:

- (a) državne [nacionalne] varnosti;
- (b) obrambe;
- (c) javne varnosti;
- (d) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;
- (e) drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo;
- (f) varstva neodvisnosti sodstva in sodnega postopka;
- (g) preprečevanja, preiskovanja, odkrivanja in pregona kršitev etike v zakonsko urejenih poklicih;
- (h) spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti v primerih iz točk (a) do (e) in (g);
- (i) varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih;
- (j) uveljavljanja civilnopravnih zahtevkov.“

15 Člen 94(2) Uredbe št. 2016/679 določa:

„Sklicevanja na razveljavljeno direktivo se štejejo kot sklicevanja na to uredbo. Sklicevanja na Delovno skupino za varstvo posameznikov pri obdelavi osebnih podatkov, ustanovljeno s členom 29 Direktive [95/46], se štejejo kot sklicevanja na Evropski odbor za varstvo podatkov, ustanovljen s to uredbo.“

Pravo Združenega kraljestva

- 16 Člen 94 Telecommunications Act 1984 (zakon o telekomunikacijah iz leta 1984) v različici, ki se uporablja za dejansko stanje v postopku v glavni stvari (v nadaljevanju: zakon iz leta 1984), naslovljen „Navodila v interesu nacionalne varnosti itd.“, določa:

„(1) Minister lahko osebi, za katero se uporablja ta člen, po posvetu z njo da splošna navodila, za katera šteje, da so nujna v interesu nacionalne varnosti ali odnosov z vlado države ali ozemlja zunaj Združenega kraljestva.

(2) Če minister meni, da je to potrebno v interesu nacionalne varnosti ali odnosov z vlado države ali ozemlja zunaj Združenega kraljestva, lahko osebi, za katero se uporablja ta člen, po posvetu z njo da navodila, v skladu s katerimi mora ta (glede na okoliščine primera) izvesti posamezno dejanje, določeno v navodilih, oziroma ga ne sme izvesti.

(2A) Minister lahko da navodila iz odstavka (1) ali (2) samo, če meni, da je ravnanje, ki se z njimi zahteva, sorazmerno s ciljem, ki se želi doseči s tem ravnanjem.

(3) Oseba, za katero se uporablja ta člen, izvede vsa navodila, ki ji jih da minister na podlagi tega člena, ne glede na katero koli drugo obveznost, ki jo ima na podlagi dela 1 ali dela 2, poglavje 1, Communications Act 2003 [(zakon o komunikacijah iz leta 2003)], in – v primeru, da so navodila dana ponudniku javnega elektronskega komunikacijskega omrežja – ne glede na to, da se nanašajo nanj v vlogi, ki ni vloga ponudnika dostopa do takega omrežja.

(4) Minister vsakemu od domov parlamenta predloži izvod vseh navodil, danih na podlagi tega člena, razen če meni, da bi bilo njihovo razkritje v nasprotju z interesi nacionalne varnosti ali odnosov z vlado države ali ozemlja zunaj Združenega kraljestva oziroma poslovnimi interesi osebe.

(5) Oseba ne sme razkriti ali biti zavezana razkriti, na podlagi zakona ali drugače, kakršnih koli informacij v zvezi z ukrepi, sprejetimi v skladu s tem členom, če jo je minister uradno obvestil o tem, da meni, da bi bilo razkritje teh informacij v nasprotju z interesi nacionalne varnosti ali odnosov z vlado države ali ozemlja zunaj Združenega kraljestva oziroma poslovnimi interesi druge osebe.

[...]

(8) Ta člen se uporablja za [Office of communications (OFCOM)] in ponudnike javnih elektronskih komunikacijskih omrežij.“

- 17 Člen 21(4) in (6) Regulation of Investigatory Powers Act 2000 (zakon o preiskovalnih pooblastilih iz leta 2000, v nadaljevanju: RIPA) določa:

„(4) ‚[K]omunikacijski podatki‘ pomenijo kar koli od tega:

- (a) vsak podatek o prometu, ki je v sporočilu ali je sporočilu priložen (s strani pošiljatelja ali kako drugače), za namene kakršne koli poštne storitve ali telekomunikacijskega sistema, s katerim se ali se lahko sporočilo prenaša;
- (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) katerega koli dela telekomunikacijskega sistema v zvezi z zagotavljanjem katere koli telekomunikacijske storitve kateri koli osebi ali v zvezi z uporabo te storitve s strani katere koli osebe;

- (c) vsako informacijo, ki ne spada pod točko (a) ali (b) in ki jo v zvezi z osebami, za katere opravlja storitev, ima ali pridobi oseba, ki zagotavlja poštno ali telekomunikacijsko storitev.

[...]

- (6) [P]ojem ‚podatek o prometu‘ v zvezi s katero koli komunikacijo [se] nanaša na:

- (a) vsak podatek, s katerim se identificira ali se lahko identificira oseba, naprava ali lokacija, na katero ali iz katere je ali je lahko sporočilo posredovano;
- (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 sporočilo posreduje;
- (c) vsak podatek, ki zajema signale za aktiviranje naprave, ki se uporablja v telekomunikacijskem sistemu za prenos sporočil; in
- (d) vsak podatek, s katerim so podatki, zajeti v posameznem sporočilu oziroma priloženi temu sporočilu, ali drugi podatki identificirani kot taki.

[...]“

- 18 Členi od 65 do 69 RIPA določajo pravila o delovanju in pristojnostih Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo). V skladu s členom 65 tega zakona je v primeru, da obstaja razlog za domnevo, da so bili podatki pridobljeni neustrezno, mogoče pri tem sodišču vložiti pritožbo.

Spor o glavni stvari in vprašanji za predhodno odločanje

- 19 V začetku leta 2015 je bila javnost seznanjena z obstojem praks zbiranja in uporabe masovnih komunikacijskih podatkov s strani različnih varnostnih in obveščevalnih agencij Združenega kraljestva, in sicer GCHQ, MI5 in MI6, med drugim s poročilom Intelligence and Security Committee of Parliament (odbor parlamenta za obveščevalne in varnostne zadeve, Združeno kraljestvo). Nevladna organizacija Privacy International je 5. junija 2015 pri Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo) vložila tožbo proti ministru za zunanje zadeve in Commonwealth, ministru za notranje zadeve ter tem varnostnim in obveščevalnim agencijam, pri čemer je izpodbijala zakonitost teh praks.
- 20 Predložitveno sodišče je preučilo zakonitost navedenih praks glede na, prvič, nacionalno pravo in določbe Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin, podpisane v Rimu 4. novembra 1950 (v nadaljevanju: EKČP), ter drugič, glede na pravo Unije. V sodbi z dne 17. oktobra 2016 je ugotovilo, da so tožene stranke v postopku v glavni stvari priznale, da so navedene varnostne in obveščevalne agencije v okviru svojih dejavnosti zbirale in uporabljale nize osebnih podatkov različnih kategorij (*bulk personal data*), kot so biografski podatki ali podatki, povezani s potovanji, finančni ali poslovni podatki, komunikacijski podatki, ki lahko vsebujejo občutljive podatke, varovane kot poklicna skrivnost, ali novinarsko gradivo. Ti podatki, ki so bili pridobljeni z različnimi, morda skrivnimi sredstvi, naj bi se analizirali z navzkrižnim preverjanjem in avtomatizirano obdelavo ter naj bi se lahko razkrili drugim osebam in organom ter delili s tujimi partnerji. V tem okviru naj bi varnostne in obveščevalne agencije uporabljale tudi masovne komunikacijske podatke, ki so bili zbrani pri ponudnikih javnih elektronskih komunikacijskih omrežij med drugim po navodilih ministrstva, sprejetih na podlagi člena 94 zakona iz leta 1984. Agenciji GCHQ in MI5 naj bi to počeli od leta 2001 oziroma 2005.

- 21 Navedeno sodišče je menilo, da so ti ukrepi zbiranja in uporabe podatkov skladni z nacionalnim pravom in – od leta 2015, s pridržkom še ne preučenih vprašanj, ki se nanašajo na sorazmernost teh ukrepov in prenos podatkov tretjim strankam – s členom 8 EKČP. V zvezi z zadnjenavedenim je to sodišče pojasnilo, da so mu bili predloženi dokazi v zvezi z jamstvi, ki se uporabljajo, zlasti kar zadeva postopke dostopa in razkritja zunaj varnostnih in obveščevalnih agencij, pogoje hrambe podatkov in obstoj neodvisnega nadzora.
- 22 Kar zadeva zakonitost ukrepov zbiranja in uporabe iz postopka v glavni stvari glede na pravo Unije, je predložitveno sodišče v sodbi z dne 8. septembra 2017 preučilo, ali ti ukrepi spadajo na področje uporabe tega prava, in če je tako, ali so združljivi s tem pravom. To sodišče je v zvezi z masovnimi komunikacijskimi podatki ugotovilo, da morajo ponudniki elektronskih komunikacijskih omrežij v skladu s členom 94 zakona iz leta 1984 v primeru, da minister da takšna navodila, varnostnim in obveščevalnim agencijam zagotoviti podatke, zbrane v okviru svoje gospodarske dejavnosti, ki spada na področje uporabe prava Unije. Vendar pa naj to ne bi veljalo za zbiranje drugih podatkov, ki jih te agencije pridobijo brez uporabe takšnih zavezujočih pooblastil. Na podlagi te ugotovitve je to sodišče menilo, da je treba Sodišču postaviti vprašanje, ali ureditev, kot je ta, ki izhaja iz člena 94, spada na področje uporabe prava Unije, in če je odgovor pritrdilen, ali in kako se za to ureditev uporabljajo zahteve iz sodne prakse, ki izhaja iz sodbe z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, v nadaljevanju: sodba Tele2, EU:C:2016:970).
- 23 V zvezi s tem predložitveno sodišče v predlogu za sprejetje predhodne odločbe navaja, da lahko minister v skladu z navedenim členom 94 ponudnikom elektronskih komunikacijskih storitev da splošna ali posebna navodila, za katera šteje, da so nujna v interesu nacionalne varnosti ali odnosov s tujo vlado. Napotuje na opredelitve pojmov iz člena 21(4) in (6) RIPA, na podlagi katerih pojasnjuje, da zadevni podatki vključujejo podatke o prometu in informacije o uporabljenih storitvah v smislu zadnjenavedene določbe, pri čemer je izključena samo vsebina sporočil. S pomočjo teh podatkov in informacij naj bi bilo zlasti mogoče dobiti odgovore na vprašanja „kdo, kje, kdaj in kako“ v zvezi s sporočilom. Navedeni podatki naj bi se posredovali varnostnim in obveščevalnim agencijam, ki naj bi jih hranile za namene svojih dejavnosti.
- 24 Po mnenju navedenega sodišča se ureditev iz postopka v glavni stvari razlikuje od ureditve, ki izhaja iz Data Retention and Investigatory Powers Act 2014 (zakon o hrambi podatkov in preiskovalnih pooblastilih iz leta 2014), ki je bil obravnavan v zadevi, v kateri je bila izdana sodba z dne 21. decembra 2016, Tele2 (C-203/15 in C-698/15, EU:C:2016:970), saj je zadnjenavedena ureditev določala hrambo podatkov s strani ponudnikov elektronskih komunikacijskih storitev in dajanje teh podatkov na voljo ne le varnostnim in obveščevalnim agencijam v interesu nacionalne varnosti, temveč tudi drugim javnim organom glede na njihove potrebe. Poleg tega naj bi se ta sodba nanašala na kazensko preiskavo, in ne na nacionalno varnost.
- 25 Predložitveno sodišče dodaja, da se podatkovne zbirke, ki jih ustvarijo varnostne in obveščevalne agencije, obdelujejo masovno in samodejno ter nespecifično, da se odkrije obstoj morebitnih neznanih groženj. V ta namen poudarja, da morajo biti tako sestavljeni nizi metapodatkov čim bolj popolni, da bi lahko razpolagali s „kopico sena“, v kateri bi našli „iglo“, ki se skriva v njej. Kar zadeva uporabnost pridobivanja masovnih podatkov s strani navedenih agencij in tehnik vpogleda vanje, navedeno sodišče napotuje zlasti na ugotovitve iz poročila z dne 19. avgusta 2016, ki ga je pripravil David Anderson, QC, tedanji United Kingdom Independent Reviewer of Terrorism Legislation (neodvisni nadzornik Združenega kraljestva za zakonodajo o terorizmu), pri čemer naj bi se oprl na preiskavo, ki jo je izvedla skupina strokovnjakov za obveščanje, ter pričevanja agentov varnostnih in obveščevalnih agencij.

- 26 Predložitveno sodišče pojasnjuje še, da po mnenju organizacije Privacy International ureditev iz postopka v glavni stvari glede na pravo Unije ni zakonita, medtem ko tožene stranke v postopku v glavni stvari menijo, da obveznost posredovanja podatkov, ki jo določa ta ureditev, dostop do teh podatkov in njihova uporaba ne spadajo na področje pristojnosti Unije zlasti v skladu s členom 4(2) PEU, v skladu s katerim nacionalna varnost ostaja v izključni pristojnosti vsake države članice.
- 27 V zvezi s tem predložitveno sodišče na podlagi sodbe z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346, točke od 56 do 59), ki se nanaša na prenos podatkov PNR (*Passenger Name Record*) zaradi varovanja javne varnosti, meni, da dejavnosti gospodarskih družb v okviru obdelave in prenosa podatkov zaradi zaščite nacionalne varnosti ne spadajo na področje uporabe prava Unije. Po njegovem mnenju ni treba preučiti, ali zadevna dejavnost pomeni obdelavo podatkov, ampak samo, ali je cilj take dejavnosti, po vsebini in učinkih, podpirati temeljno državno funkcijo v smislu člena 4(2) PEU prek okvira, ki ga določijo javni organi in se nanaša na javno varnost.
- 28 Če bi ukrepi iz postopka v glavni stvari vseeno spadali na področje uporabe prava Unije, predložitveno sodišče meni, da se zahteve iz točk od 119 do 125 sodbe z dne 21. decembra 2016, Tele2 (C-203/15 in C-698/15, EU:C:2016:970), izkažejo za neprimerne v okviru nacionalne varnosti in bi spodbile zmožnost varnostnih in obveščevalnih agencij, da se spopadejo z nekaterimi grožnjami za nacionalno varnost.
- 29 V teh okoliščinah je Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili) prekinilo odločanje in Sodišču v predhodno odločanje predložilo ti vprašanji:

„V okoliščinah, v katerih:

- (a) je zmožnost [varnostnih in obveščevalnih agencij], da uporabljajo posredovane jim [masovne komunikacijske podatke], bistvena za varovanje nacionalne varnosti Združenega kraljestva, vključno na področju boja proti terorizmu, protiobveščevalni dejavnosti in širjenju jedrskega orožja;
 - (b) je temeljna značilnost uporabe [masovnih komunikacijskih podatkov] s strani [varnostnih in obveščevalnih agencij] odkrivanje prej neznanih groženj nacionalni varnosti s tehnikami neusmerjenega zbiranja, ki temeljijo na zbiranju [masovnih komunikacijskih podatkov] na enem mestu. Glavna uporabnost tega je hitro identificiranje in razvoj ciljev ter zagotavljanje podlage za ukrepanje ob neposrednih grožnjah;
 - (c) se od ponudnika elektronskega komunikacijskega omrežja nato ne zahteva hramba [masovnih komunikacijskih podatkov] (za dalj časa kot pri običajnem poslovanju), ki jih hrani izključno država ([varnostne in obveščevalne agencije]);
 - (d) je nacionalno sodišče (z nekaterimi pridržanimi vprašanji) presodilo, da so jamstva v zvezi z uporabo [masovnih komunikacijskih podatkov] s strani [varnostnih in obveščevalnih agencij] skladna z zahtevami EKČP; in
 - (e) je nacionalno sodišče presodilo, da bi se z naložitvijo zahtev iz točk od 119 do 125 sodbe [z dne 21. decembra 2016, Tele2 (C-203/15 in C-698/15, EU:C:2016:970)], če se uporabljajo, ogrozili ukrepi [varnostnih in obveščevalnih agencij] za varovanje nacionalne varnosti, s tem pa bi se ogrozila nacionalna varnost Združenega kraljestva;
1. Ali ob upoštevanju člena 4 PEU in člena 1(3) Direktive [2002/58] zahteva v navodilu [ministra], da mora ponudnik elektronskega komunikacijskega omrežja varnostnim in obveščevalnim agencijam [...] države članice posredovati masovne 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 [ministra] uporabljajo katere od zahtev[, ki se uporabljajo za hranjene komunikacijske podatke in ki so določene v točkah od 119 do 125 sodb z dne 21. decembra 2016, Tele2 (C-203/15 in C-698/15, EU:C:2016:970),] ali katere druge zahteve poleg tistih iz EKČP? In če se, kako in v kakšnem obsegu se take zahteve uporabljajo ob upoštevanju bistvene potrebe [varnostnih in obveščevalnih agencij], da uporabljajo tehnike masovnega 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?“

Vprašanja za predhodno odločanje

Prvo vprašanje

- 30 Predložitveno sodišče s prvim vprašanjem v bistvu sprašuje, ali je treba člen 1(3) Direktive 2002/58 v povezavi s členom 4(2) PEU razlagati tako, da nacionalna ureditev, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži, da podatke o prometu in podatke o lokaciji posredujejo varnostnim in obveščevalnim agencijam, spada na področje uporabe te direktive.
- 31 V zvezi s tem organizacija Privacy International v bistvu trdi, da glede na spoznanja, ki izhajajo iz sodne prakse Sodišča, kar zadeva področje uporabe Direktive 2002/58, tako zbiranje podatkov od teh ponudnikov s strani varnostnih in obveščevalnih agencij v skladu s členom 94 zakona iz leta 1984 kot njihova uporaba s strani teh agencij spadata na področje uporabe te direktive, ne glede na to, ali se ti podatki zberejo z naknadnim posredovanjem ali se zbirajo sproti. Natančneje, dejstvo, da je cilj zaščite nacionalne varnosti izrecno naveden v členu 15(1) navedene direktive, naj ne bi pomenilo, da se ta direktiva v takšnih položajih ne uporablja, člen 4(2) PEU pa naj ne bi vplival na to presojo.
- 32 Vlada Združenega kraljestva, češka in estonska vlada, Irska ter francoska, ciprska, madžarska, poljska in švedska vlada pa v bistvu trdijo, da se Direktiva 2002/58 ne uporablja za nacionalno zakonodajo iz postopka v glavni stvari, ker je namen te zakonodaje zaščita nacionalne varnosti. Dejavnosti varnostnih in obveščevalnih agencij naj bi spadale med bistvene funkcije držav članic, katerih namen je vzdrževanje javnega reda ter zagotavljanje notranje varnosti in ozemeljske celovitosti, in naj bi bile zato v izključni pristojnosti držav članic, kot naj bi bilo razvidno med drugim iz člena 4(2), tretji stavek, PEU.
- 33 Po navedbah teh vlad Direktive 2002/58 torej ni mogoče razlagati tako, da nacionalni ukrepi za zaščito nacionalne varnosti spadajo na njeno področje uporabe. To področje uporabe naj bi določal člen 1(3) te direktive, ki naj bi z njega izključeval, kot je bilo to določeno že v členu 3(2), prva alineja, Direktive 95/46, dejavnosti, povezane z javno varnostjo, obrambo in državno varnostjo. Te določbe naj bi odražale razdelitev pristojnosti, določenih v členu 4(2) PEU, in odvzet naj bi jim bil polni učinek, če bi ukrepi s področja nacionalne varnosti morali izpolnjevati zahteve iz Direktive 2002/58. Poleg tega naj bi bilo mogoče sodno prakso Sodišča, ki izhaja iz sodb z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346), ki se nanaša na člen 3(2), prva alineja, Direktive 95/46, uporabiti za člen 1(3) Direktive 2002/58.
- 34 V zvezi s tem je treba navesti, da Direktiva 2002/58 v skladu s svojim členom 1(1) med drugim določa harmonizacijo nacionalnih določb, ki so potrebne za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij.

- 35 Člen 1(3) te direktive s področja uporabe te direktive izključuje „dejavnosti države“ na področjih, ki so v njem navedena, med katerimi so dejavnosti na področju kazenskega prava ter dejavnosti v zvezi z javno varnostjo, obrambo in državno varnostjo, vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo. Dejavnosti, ki so tako navedene kot primer, so vedno dejavnosti držav ali državnih organov, ki niso povezane s področji dejavnosti posameznikov (sodba z dne 2. oktobra 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, točka 32 in navedena sodna praksa).
- 36 Poleg tega člen 3 Direktive 2002/58 določa, da se ta direktiva uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave (v nadaljevanju: elektronske komunikacijske storitve). Zato je treba šteti, da navedena direktiva ureja dejavnosti ponudnikov teh storitev (sodba z dne 2. oktobra 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, točka 33 in navedena sodna praksa).
- 37 V tem okviru člen 15(1) Direktive 2002/58 določa, da lahko države članice, ob upoštevanju pogojev, ki jih določa, sprejmejo „zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive“ (sodba z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točka 71).
- 38 Člen 15(1) Direktive 2002/58 pa nujno zahteva, da nacionalni zakonski ukrepi, ki so v njem navedeni, spadajo na področje uporabe te direktive, ker ta državam članicam izrecno dopušča, da te ukrepe sprejmejo le ob upoštevanju pogojev, ki jih določa. Poleg tega taki ukrepi za namene, navedene v tej določbi, urejajo dejavnost ponudnikov elektronskih komunikacijskih storitev (sodba z dne 2. oktobra 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, točka 34 in navedena sodna praksa).
- 39 Sodišče je zlasti glede na te ugotovitve razsodilo, da je treba člen 15(1) Direktive 2002/58 v povezavi s členom 3 te direktive razlagati tako, da na področje uporabe te direktive zlasti spada ne le zakonski ukrep, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da hranijo podatke o prometu in podatke o lokaciji, temveč tudi zakonski ukrep, s katerim jim je naloženo, da pristojnim nacionalnim organom odobrijo dostop do teh podatkov. Taki zakonski ukrepi namreč nujno vključujejo obdelavo teh podatkov s strani navedenih ponudnikov in jih v delu, v katerem urejajo dejavnosti navedenih dobaviteljev, ni mogoče šteti za dejavnosti držav iz člena 1(3) navedene direktive (glej v tem smislu sodbo z dne 2. oktobra 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, točki 35 in 37 ter navedena sodna praksa).
- 40 Kar zadeva zakonski ukrep, kot je člen 94 zakona iz leta 1984, na podlagi katerega lahko pristojni organ ponudnikom elektronskih komunikacijskih storitev da navodilo za razkritje s posredovanjem masovnih komunikacijskih podatkov varnostnim in obveščevalnim agencijam, je treba poudariti, da v skladu z opredelitvijo iz člena 4, točka 2, Uredbe št. 2016/679, ki se uporablja v skladu s členom 2 Direktive 2002/58 v povezavi s členom 94(2) navedene uredbe, pojem „obdelava osebnih podatkov“ pomeni „vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, [...] shranjevanje, [...] vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa [...]“.
- 41 Iz tega sledi, da razkritje osebnih podatkov s posredovanjem, tako kot shranjevanje podatkov ali kakršna koli druga oblika omogočanja dostopa, pomeni obdelavo v smislu člena 3 Direktive 2002/58 in zato spada na področje uporabe te direktive (glej v tem smislu sodbo z dne 29. januarja 2008, *Promusicae*, C-275/06, EU:C:2008:54, točka 45).
- 42 Poleg tega bi glede na ugotovitve iz točke 38 te sodbe in glede na splošno sistematiko Direktive 2002/58 razlaga te direktive, v skladu s katero bi bili zakonski ukrepi iz njenega člena 15(1) izključeni s področja uporabe navedene direktive, ker se cilji, ki jim morajo ti ukrepi slediti, v bistvenem

prekrivajo z nameni, ki jih uresničujejo dejavnosti iz člena 1(3) te direktive, temu členu 15(1) odvzela polni učinek (glej v tem smislu sodbo z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točki 72 in 73).

- 43 Pojma „dejavnosti“ iz člena 1(3) Direktive 2002/58 torej ni mogoče – kot je v bistvu navedel generalni pravobranilec v točki 75 sklepnih predlogov v združenih zadevah *La Quadrature du Net* in drugi (C-511/18 in C-512/18, EU:C:2020:6), na katere napotuje v točki 24 sklepnih predlogov v tej zadevi – razlagati tako, da zajema zakonske ukrepe iz člena 15(1) te direktive.
- 44 Določbe člena 4(2) PEU, na katere se sklicujejo vlade, navedene v točki 32 te sodbe, ne morejo ovreči te ugotovitve. V skladu z ustaljeno sodno prakso Sodišča namreč, čeprav so države članice pristojne, da opredelijo svoje bistvene varnostne interese in sprejmejo primerne ukrepe za zagotovitev svoje notranje in zunanje varnosti, zgolj dejstvo, da je bil nacionalni ukrep sprejet zaradi zaščite nacionalne varnosti, ne more povzročiti izključitve uporabe prava Unije in držav članic oprostiti obveznosti spoštovanja tega prava (glej v tem smislu sodbe z dne 4. junija 2013, *ZZ*, C-300/11, EU:C:2013:363, točka 38 in navedena sodna praksa; z dne 20. marca 2018, *Komisija/Avstrija* (Državna tiskarna), C-187/16, EU:C:2018:194, točki 75 in 76, in z dne 2. aprila 2020, *Komisija/Poljska, Madžarska in Češka republika* (Začasni mehanizem za premestitev prosilcev za mednarodno zaščito), C-715/17, C-718/17 in C-719/17, EU:C:2020:257, točki 143 in 170).
- 45 Res je, da je Sodišče v sodbi z dne 30. maja 2006, *Parlament/Svet in Komisija* (C-317/04 in C-318/04, EU:C:2006:346, točke od 56 do 59), razsodilo, da prenos osebnih podatkov s strani letalskih družb javnim organom tretje države zaradi preprečevanja terorizma in drugih hudih kaznivih dejanj ter boja proti njim v skladu s členom 3(2), prva alineja, Direktive 95/46 ne spada na področje uporabe te direktive, ker tak prenos spada v okvir, ki ga določijo javni organi in se nanaša na javno varnost.
- 46 Vendar glede na ugotovitve iz točk 36, 38 in 39 te sodbe te sodne prakse ni mogoče uporabiti pri razlagi člena 1(3) Direktive 2002/58. Kot je namreč generalni pravobranilec v bistvu navedel v točkah od 70 do 72 sklepnih predlogov v združenih zadevah *La Quadrature du Net* in drugi (C-511/18 in C-512/18, EU:C:2020:6), so s členom 3(2), prva alineja, Direktive 95/46, na katerega se nanaša navedena sodna praksa, s področja uporabe zadnjenavedene direktive na splošno izključeni „postopk[i] obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo“, brez razlikovanja glede na to, kdo izvaja zadevno obdelavo podatkov. V okviru razlage člena 1(3) Direktive 2002/58 pa je tako razlikovanje potrebno. Kot izhaja iz točk od 37 do 39 in 42 te sodbe, namreč vsi postopki obdelave osebnih podatkov, ki jih izvajajo ponudniki elektronskih komunikacijskih storitev, spadajo na področje uporabe navedene direktive, vključno s tistimi, ki izhajajo iz obveznosti, ki jih tem ponudnikom naložijo javni organi, medtem ko bi zadnjenavedeni postopki obdelave, glede na okoliščine primera, lahko spadali na področje uporabe izjeme iz člena 3(2), prva alineja, Direktive 95/46 ob upoštevanju širšega besedila te določbe, ki zajema vse postopke obdelave v zvezi z javno varnostjo, obrambo ali državno varnostjo, ne glede na to, kdo jih izvaja.
- 47 Poleg tega je treba poudariti, da je bila Direktiva 95/46, ki je bila predmet zadeve, v kateri je bila izdana sodba z dne 30. maja 2006, *Parlament/Svet in Komisija* (C-317/04 in C-318/04, EU:C:2006:346), na podlagi člena 94(1) Uredbe 2016/679 razveljavljena in nadomeščena s to uredbo z učinkom od 25. maja 2018. Čeprav navedena uredba v členu 2(2)(d) določa, da se ne uporablja za obdelavo „s strani pristojnih organov“ za namene, med drugim, preprečevanja in odkrivanja kaznivih dejanj, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, pa iz člena 23(1)(d) in (h) te uredbe izhaja, da obdelava osebnih podatkov, ki jo v iste namene izvajajo posamezniki, spada na njeno področje uporabe. Iz tega sledi, da je zgoraj navedena razlaga člena 1(3), člena 3 in člena 15(1) Direktive 2002/58 skladna z opredelitvijo področja uporabe Uredbe 2016/679, ki ga dopolnjuje in podrobno določa ta direktiva.

- 48 Kadar pa države članice neposredno izvajajo ukrepe, ki odstopajo od načela zaupnosti elektronskih komunikacij, ne da bi ponudnikom takih komunikacijskih storitev naložile obveznosti obdelave, varstvo podatkov zadevnih oseb ne spada na področje uporabe Direktive 2002/58, temveč zgolj na področje uporabe nacionalnega prava, s pridržkom uporabe Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL 2016, L 119, str. 89), tako da morajo biti zadevni ukrepi skladni med drugim z nacionalnim ustavnim pravom in zahtevami iz EKČP.
- 49 Ob upoštevanju navedenega je treba na prvo vprašanje odgovoriti, da je treba člen 1(3), člen 3 in člen 15(1) Direktive 2002/58 v povezavi s členom 4(2) PEU razlagati tako, da nacionalna ureditev, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži, da podatke o prometu in podatke o lokaciji posredujejo varnostnim in obveščevalnim agencijam, spada na področje uporabe te direktive.

Drugo vprašanje

- 50 Predložitveno sodišče z drugim vprašanjem v bistvu sprašuje, ali je treba člen 15(1) Direktive 2002/58 v povezavi s členom 4(2) PEU ter členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži splošno in neselektivno posredovanje podatkov o prometu in podatkov o lokaciji varnostnim in obveščevalnim agencijam.
- 51 Uvodoma je treba opozoriti, da v skladu z navedbami v predlogu za sprejetje predhodne odločbe člen 94 zakona iz leta 1984 dovoljuje ministru, da ponudnikom elektronskih komunikacijskih storitev prek navodil naloži – kadar meni, da je to nujno v interesu nacionalne varnosti ali odnosov s tujo vlado – da varnostnim in obveščevalnim agencijam posredujejo masovne komunikacijske podatke, pri čemer ti v skladu s členom 21(4) in (6) RIPA vključujejo podatke o prometu in podatke o lokaciji ter informacije o uporabljenih storitvah. V zadnjenavedeni določbi so med drugim zajeti podatki, ki so potrebni za prepoznavo vira in cilja sporočila, določitev datuma, ure, trajanja in vrste sporočila, prepoznavo uporabljene opreme ter ugotovitev lokacije terminalske opreme in sporočila, med katerimi so predvsem ime in naslov uporabnika, telefonska številka klicatelja in klicana telefonska številka, naslova IP vira in cilja sporočila ter naslovi obiskanih spletnih strani.
- 52 Takšno razkritje podatkov s posredovanjem zadeva vse uporabnike elektronskih komunikacijskih sredstev, pri čemer ni pojasnjeno, ali se mora to posredovanje izvajati sproti ali naknadno. Po navedbah v predlogu za sprejetje predhodne odločbe posredovane podatke nato hranijo varnostne in obveščevalne agencije, ki jim ti podatki ostanejo na razpolago za namene njihovih dejavnosti, tako kot druge podatkovne zbirke, ki jih vodijo. Natančneje, tako zbrani podatki, ki so predmet masovne samodejne obdelave in analize, se lahko navzkrižno preverjajo z drugimi podatkovnimi zbirkami, ki vsebujejo različne kategorije masovnih osebnih podatkov, ali razkrijejo zunaj teh agencij in tretjim državam. Končno, ti postopki ne zahtevajo predhodnega dovoljenja sodišča ali neodvisnega upravnega organa in ne vključujejo nikakršnega obveščanja zadevnih oseb.
- 53 Namen Direktive 2002/58 je, kot izhaja med drugim iz njenih uvodnih izjav 6 in 7, zavarovati uporabnike elektronskih komunikacijskih storitev pred tveganji za njihove osebne podatke in zasebnost, ki izhajajo iz novih tehnologij in zlasti čedalje večje zmogljivosti samodejnega shranjevanja in obdelave. Zlasti pa je namen navedene direktive, kot je navedeno v njeni uvodni izjavi 2, zagotoviti polno spoštovanje pravic, določenih v členih 7 in 8 Listine. V zvezi s tem iz obrazložitve predloga Direktive Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (COM(2000) 385 final), na podlagi katerega je bila sprejeta

Direktiva 2002/58, izhaja, da je zakonodajalec Unije želel „še naprej zagotavljati visoko raven varstva osebnih podatkov in zasebnosti za vse elektronske komunikacijske storitve ne glede na tehnologijo, ki se uporablja“.

- 54 V zvezi s tem člen 5(1) Direktive 2002/58 določa, da „[d]ržave članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev“. V tej določbi je tudi poudarjeno, da „[države članice] [z]lasti prepovejo vsem osebam razen uporabnikom, da poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1)“, ter določeno, da „[t]a odstavek ne preprečuje tehničnega shranjevanja, ki je potrebno za prenos sporočila, brez vpliva na načelo zaupnosti“.
- 55 Navedeni člen 5(1) torej določa načelo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu ter med drugim zahteva, da se načeloma vsem razen uporabnikom prepove shranjevanje teh sporočil in podatkov brez privolitve uporabnikov. Ta določba glede na svoje splošno besedilo nujno zajema vse postopke, ki tretjim osebam omogočajo, da se seznanijo s sporočili in z njimi povezanimi podatki za namene, ki niso prenos sporočila.
- 56 Prepoved prestrezanja sporočil in z njimi povezanih podatkov iz člena 5(1) Direktive 2002/58 torej zajema vse oblike dajanja podatkov o prometu in podatkov o lokaciji na razpolago javnim organom, kot so varnostne in obveščevalne agencije, s strani ponudnikov elektronskih komunikacijskih storitev kot tudi shranjevanje teh podatkov s strani teh organov, ne glede na njihovo nadaljnjo uporabo.
- 57 Zakonodajalec Unije je tako s sprejetjem te direktive konkretiziral pravice, določene v členih 7 in 8 Listine, tako da uporabniki elektronskih komunikacijskih sredstev načeloma upravičeno pričakujejo, da bodo njihova sporočila in z njimi povezani podatki, če ne privolijo v nasprotno, ostali anonimni in jih ne bo mogoče shraniti (sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi, C-511/18, C-512/18 in C-520/18, točka 109).
- 58 Vendar imajo države članice na podlagi člena 15(1) Direktive 2002/58 možnost, da določijo izjeme od načelne obveznosti, določene v členu 5(1) te direktive, da zagotavljajo zaupnost osebnih podatkov, in od ustreznih obveznosti, določenih predvsem v členih 6 in 9 navedene direktive, če je taka omejitev potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito nacionalne varnosti, obrambe in javne varnosti ali za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo hrambo podatkov za omejeno obdobje, če je to upravičeno iz katerega od teh razlogov.
- 59 Vendar možnost odstopanja od pravic in obveznosti iz členov 5, 6 in 9 Direktive 2002/58 ne more upravičiti tega, da odstopanje od načelne obveznosti zagotavljanja zaupnosti elektronskih komunikacij in z njimi povezanih podatkov ter zlasti od prepovedi shranjevanja teh podatkov, ki je izrecno določena v členu 5 te direktive, postane pravilo (glej v tem smislu sodbi z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 89 in 104, in z dne 6. oktobra 2020, La Quadrature du Net in drugi, C-511/18, C-512/18 in C-520/18, točka 111).
- 60 Poleg tega je iz člena 15(1), tretji stavek, Direktive 2002/58 razvidno, da lahko države članice zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členih 5, 6 in 9 te direktive, sprejmejo le ob upoštevanju splošnih načel prava Unije, med katerimi je načelo sorazmernosti, in temeljnih pravic, zagotovljenih z Listino. V zvezi s tem je Sodišče že razsodilo, da se z obveznostjo, ki jo država članica z nacionalno ureditvijo naloži ponudnikom elektronskih komunikacijskih storitev, in sicer da hranijo podatke o prometu, da se, če je to potrebno, pristojnim nacionalnim organom omogoči dostop do teh podatkov, postavljajo vprašanja v zvezi s spoštovanjem ne le členov 7 in 8 Listine, ki se nanašata na varstvo zasebnega življenja in varstvo osebnih podatkov, ampak tudi člena 11

Listine, ki se nanaša na svobodo izražanja (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 25 in 70, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 91 in 92 ter navedena sodna praksa).

- 61 Ista vprašanja se postavljajo tudi za druge vrste obdelave podatkov, kot je njihov prenos osebam, ki niso uporabniki, ali dostop do teh podatkov za njihovo uporabo (glej po analogiji mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 122 in 123 ter navedena sodna praksa).
- 62 Pri razlagi člena 15(1) Direktive 2002/58 je treba torej upoštevati tako pomembnost pravice do spoštovanja zasebnega življenja, ki jo zagotavlja člen 7 Listine, in pravice do varstva osebnih podatkov, ki jo zagotavlja člen 8 Listine, kot izhaja iz sodne prakse Sodišča, kot tudi pravice do svobode izražanja, glede na to, da je zadnjenavedena temeljna pravica, zagotovljena v členu 11 Listine, eden od glavnih temeljev demokratične in pluralistične družbe ter je del vrednot, na katerih v skladu s členom 2 PEU temelji Unija (glej v tem smislu sodbi z dne 6. marca 2001, Connolly/Komisija, C-274/99 P, EU:C:2001:127, točka 39, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 93 in navedena sodna praksa).
- 63 Vendar pravice iz členov 7, 8 in 11 Listine niso absolutne, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi (glej v tem smislu sodbo z dne 16. julija 2020, Facebook Ireland in Schrems, C-311/18, EU:C:2020:559, točka 172 in navedena sodna praksa).
- 64 Kot namreč izhaja iz člena 52(1) Listine, ta dopušča omejitve pri uresničevanju teh pravic, če so te omejitve predpisane z zakonom, če spoštujejo bistveno vsebino teh pravic, če so ob upoštevanju načela sorazmernosti potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih.
- 65 Dodati je treba, da zahteva, da mora biti kakršno koli omejevanje uresničevanja temeljnih pravic predpisano z zakonom, pomeni, da mora biti že v pravni podlagi, ki omogoča poseg v te pravice, opredeljen obseg omejitve uresničevanja zadevne pravice (sodba z dne 16. julija 2020, Facebook Ireland in Schrems, C-311/18, EU:C:2020:559, točka 175 in navedena sodna praksa).
- 66 Kar zadeva spoštovanje načela sorazmernosti, člen 15(1), prvi stavek, Direktive 2002/58 določa, da lahko države članice sprejmejo ukrep, ki odstopa od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, kadar je tak ukrep „potrben, primeren in ustrezen [...] znotraj demokratične družbe“ glede na cilje te določbe. V uvodni izjavi 11 te direktive je pojasnjeno, da mora biti tak ukrep „dosledno“ sorazmeren z namenom.
- 67 V zvezi s tem je treba opozoriti, da varstvo temeljne pravice do spoštovanja zasebnega življenja v skladu z ustaljeno sodno prakso Sodišča zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno. Poleg tega cilja v splošnem interesu ni mogoče uresničevati brez upoštevanja dejstva, da ga je treba uskladiti s temeljnimi pravicami, na katere se nanaša ukrep, in sicer z uravnoteženjem cilja ter zadevnih interesov in pravic (glej v tem smislu sodbe z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia, C-73/07, EU:C:2008:727, točka 56; z dne 9. novembra 2010, Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, EU:C:2010:662, točke 76, 77 in 86, ter z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 52; mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 140).
- 68 Za izpolnitev zahteve po sorazmernosti mora ureditev določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe. Ta ureditev mora biti zakonsko zavezujoča v nacionalnem pravu, v njej pa mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa

obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno. Nujnost obstoja takih jamstev je toliko pomembnejša, če se osebni podatki obdelujejo samodejno, zlasti kadar obstaja veliko tveganje nezakonitega dostopa do teh podatkov. Te ugotovitve veljajo še posebej, kadar gre za varstvo te posebne kategorije osebnih podatkov, ki so občutljivi (glej v tem smislu sodbi z dne 8. aprila 2014, *Digital Rights Ireland* in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 54 in 55, in z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točka 117; mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 141).

- 69 Kar zadeva vprašanje, ali nacionalna ureditev, kakršna je ta v postopku v glavni stvari, izpolnjuje zahteve iz člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine, je treba poudariti, da prenos podatkov o prometu in podatkov o lokaciji osebam, ki niso uporabniki, kot so varnostne in obveščevalne agencije, odstopa od načela zaupnosti. Če se ta postopek, tako kot v obravnavanem primeru, izvaja splošno in neselektivno, postane odstopanje od načelne obveznosti zagotavljanja zaupnosti podatkov pravilo, medtem ko sistem, uveden z Direktivo 2002/58, zahteva, da takšno odstopanje ostane izjema.
- 70 Poleg tega v skladu z ustaljeno sodno prakso Sodišča prenos podatkov o prometu in podatkov o lokaciji tretjemu pomeni poseg v temeljne pravice iz členov 7 in 8 Listine, ne glede na nadaljnjo uporabo teh podatkov. Glede tega ni pomembno, ali so zadevne informacije o zasebnem življenju občutljive, niti to, ali so bile zadevne osebe zaradi tega poseganja morda oškodovane (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 124 in 126 ter navedena sodna praksa, in sodbo z dne 6. oktobra 2020, *La Quadrature du Net* in drugi, C-511/18, C-512/18 in C-520/18, točki 115 in 116).
- 71 Poseg, ki ga pomeni prenos podatkov o prometu in podatkov o lokaciji varnostnim in obveščevalnim agencijam, v pravico, določeno v členu 7 Listine, je treba obravnavati kot posebno resen, zlasti ob upoštevanju občutljivosti informacij, ki jih lahko zagotovijo ti podatki, in še posebej možnosti, da se na njihovi podlagi ugotovi profil zadevnih oseb, saj so take informacije prav tako občutljive kot sama vsebina sporočil. Poleg tega lahko ta poseg pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje (glej po analogiji sodbi z dne 8. aprila 2014, *Digital Rights Ireland* in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 27 in 37, in z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točki 99 in 100).
- 72 Opozoriti je treba še, da lahko prenos podatkov o prometu in podatkov o lokaciji javnim organom za varnostne namene sam po sebi posega v pravico do spoštovanja komunikacij, določeno v členu 7 Listine, in odvrča uporabnike elektronskih komunikacijskih sredstev od uresničevanja svobode izražanja, ki je zagotovljena s členom 11 Listine. Takšni odvrčalni učinki lahko vplivajo zlasti na osebe, za komunikacije katerih velja v skladu z nacionalnimi predpisi poklicna skrivnost, in za žvižgače, katerih dejavnosti so zaščitene z Direktivo (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (UL 2019, L 305, str. 17). Poleg tega so ti učinki toliko resnejši, kolikor večja sta število in raznovrstnost hranjenih podatkov (glej v tem smislu sodbe z dne 8. aprila 2014, *Digital Rights Ireland* in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 28; z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točka 101, in z dne 6. oktobra 2020, *La Quadrature du Net* in drugi, C-511/18, C-512/18 in C-520/18, točka 118).
- 73 Nazadnje, glede na veliko količino podatkov o prometu in o lokaciji, ki se s splošnim ukrepom shranjevanja lahko neprekinjeno shranjuje, in glede na občutljivost informacij, ki se lahko zagotovijo s temi podatki, že samo shranjevanje navedenih podatkov pri ponudnikih elektronskih komunikacijskih storitev vključuje tveganje zlorabe in nezakonitega dostopa.

- 74 Kar zadeva cilje, ki lahko upravičujejo takšne posege, zlasti cilj zaščite nacionalne varnosti iz postopka v glavni stvari, je treba najprej poudariti, da člen 4(2) PEU določa, da nacionalna varnost ostaja v izključni pristojnosti vsake države članice. Ta pristojnost ustreza glavnemu interesu, ki je zaščititi bistvene funkcije države in temeljne interese družbe, ter vključuje preprečevanje in kaznovanje dejavnosti, ki lahko resno destabilizirajo temeljne ustavne, politične, gospodarske ali družbene strukture države ter zlasti neposredno ogrozijo družbo, prebivalstvo ali državo kot tako, kot so zlasti teroristična dejanja (sodba z dne 6. oktobra 2020, *La Quadrature du Net* in drugi, C-511/18, C-512/18 in C-520/18, točka 135).
- 75 Vendar pa je cilj zaščite nacionalne varnosti, kot izhaja iz člena 4(2) PEU, pomembnejši od drugih ciljev, navedenih v členu 15(1) Direktive 2002/58, med drugim od ciljev boja proti kriminalu na splošno, tudi hudemu, in zaščite javne varnosti. Grožnje, kot so navedene v prejšnji točki, se namreč po naravi in posebni resnosti razlikujejo od splošnega tveganja, da se pojavijo napetosti ali nemiri, tudi hudi, ki bi ogrozili javno varnost. S pridržkom upoštevanja drugih zahtev iz člena 52(1) Listine je torej s ciljem zaščite nacionalne varnosti mogoče utemeljiti ukrepe, ki pomenijo poseg v temeljne pravice, ki je resnejši od tistega, ki bi ga bilo mogoče utemeljiti s temi drugimi cilji (sodba z dne 6. oktobra 2020, *La Quadrature du Net* in drugi, C-511/18, C-512/18 in C-520/18, točka 136).
- 76 Vendar pa mora nacionalna zakonodaja, ki posega v temeljne pravice, določene v členih 7 in 8 Listine – da bi bila izpolnjena zahteva po sorazmernosti iz točke 67 te sodbe, v skladu s katero morajo biti odstopanja in omejitve pri varstvu osebnih podatkov strogo omejeni na tisto, kar je nujno – izpolnjevati zahteve, ki izhajajo iz sodne prakse, navedene v točkah 65, 67 in 68 te sodbe.
- 77 Natančneje, kar zadeva dostop organa do osebnih podatkov, ureditev ne more zgolj zahtevati, da dostop organov do podatkov ustreza cilju, ki mu sledi ta ureditev, temveč mora določati tudi materialne in postopkovne pogoje za to uporabo (glej po analogiji mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 192 in navedena sodna praksa).
- 78 Ker torej ni mogoče šteti, da je splošni dostop do vseh hranjenih podatkov ob neobstoju kakršne koli povezave, tudi posredne, s ciljem, ki se mu sledi, omejen na nujno potrebno, se mora nacionalna ureditev, ki ureja dostop do podatkov o prometu in lokaciji, pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do zadevnih podatkov, opreti na objektivna merila (glej v tem smislu sodbo z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točka 119 in navedena sodna praksa).
- 79 Navedene zahteve veljajo še toliko bolj za zakonski ukrep, kot je ta v postopku v glavni stvari, na podlagi katerega lahko pristojni nacionalni organ ponudnikom elektronskih komunikacijskih storitev naloži, da s splošnim in neselektivnim posredovanjem varnostnim in obveščevalnim agencijam razkrijejo podatke o prometu in podatke o lokaciji. S takim posredovanjem se namreč ti podatki dajo na razpolago javnim organom (glej po analogiji mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 212).
- 80 Ker se posredovanje podatkov o prometu in podatkov o lokaciji izvaja splošno in neselektivno, na splošno zadeva vse osebe, ki uporabljajo elektronske komunikacijske storitve. Uporablja se torej tudi za osebe, v zvezi s katerimi ni nobenega indika, na podlagi katerega bi bilo mogoče sklepati, da obstaja povezava, čeprav posredna ali daljna, med njihovim ravnanjem in ciljem zaščite nacionalne varnosti, ter zlasti ne da bi bila ugotovljena povezava med podatki, katerih posredovanje je določeno, in grožnja za nacionalno varnost (glej v tem smislu sodbi z dne 8. aprila 2014, *Digital Rights Ireland* in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 57 in 58, in z dne 21. decembra 2016, *Tele2*, C-203/15 in C-698/15, EU:C:2016:970, točka 105). Glede na to, da je posredovanje takšnih podatkov javnim organom v skladu s tem, kar je bilo ugotovljeno v točki 79 te sodbe, enakovredno dostopu, je treba šteti, da ima ureditev, ki omogoča splošno in neselektivno posredovanje podatkov javnim organom, za posledico splošen dostop.

- 81 Iz tega izhaja, da nacionalna ureditev, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da s splošnim in neselektivnim posredovanjem varnostnim in obveščevalnim agencijam razkrijejo podatke o prometu in podatke o lokaciji, presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 v povezavi s členom 4(2) PEU ter členi 7, 8, 11 in 52(1) Listine.
- 82 Glede na vse zgoraj navedeno je treba na drugo vprašanje odgovoriti, da je treba člen 15(1) Direktive 2002/58 v povezavi s členom 4(2) PEU ter členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži splošno in neselektivno posredovanje podatkov o prometu in podatkov o lokaciji varnostnim in obveščevalnim agencijam.

Stroški

- 83 Ker je ta postopek za stranke v postopku v glavni stvari ena od stopenj v postopku pred predložitvenim sodiščem, to odloči o stroških. Stroški za predložitev stališč Sodišču, ki niso stroški omenjenih strank, se ne povrnejo.

Iz teh razlogov je Sodišče (veliki senat) razsodilo:

1. Člen 1(3), člen 3 in člen 15(1) 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), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, v povezavi s členom 4(2) PEU je treba razlagati tako, da nacionalna ureditev, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži, da podatke o prometu in podatke o lokaciji posredujejo varnostnim in obveščevalnim agencijam, spada na področje uporabe te direktive.
2. Člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členom 4(2) PEU ter členi 7, 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da nasprotuje nacionalni ureditvi, ki državnemu organu omogoča, da zaradi zaščite nacionalne varnosti ponudnikom elektronskih komunikacijskih storitev naloži splošno in neselektivno posredovanje podatkov o prometu in podatkov o lokaciji varnostnim in obveščevalnim agencijam.

Podpisi