Zbornik sudske prakse

PRESUDA SUDA (veliko vijeće)

6. listopada 2020.*

„Zahtjev za prethodnu odluku – Obrada osobnih podataka u području elektroničkih komunikacija – Pružatelji elektroničkih komunikacijskih usluga – Opći i neselektivni prijenos podataka o prometu i lokaciji – Zaštita nacionalne sigurnosti – Direktiva 2002/58/EZ – Područje primjene – Članak 1. stavak 3. i članak 3. – Povjerljivost elektroničkih komunikacija – Zaštita – Članak 5. i članak 15. stavak 1. – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 11. te članak 52. stavak 1. – Članak 4. stavak 2. UEU-a”

U predmetu C-623/17,

povodom zahtjeva za prethodnu odluku na temelju članka 267. UFEU-a, koji je uputio Investigatory Powers Tribunal (Sud za istražne ovlasti, Ujedinjena Kraljevina), odlukom od 18. listopada 2017., koju je Sud zaprimio 31. listopada 2017., u postupku

Privacy International

protiv

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

SUD (veliko vijeće),

u sastavu: K. Lenaerts, predsjednik, R. Silva de Lapuerta, potpredsjednica, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb i L. S. Rossi, predsjednici vijeća, J. Malenovský, L. Bay Larsen, T. von Danwitz (izvjestitelj), C. Toader, K. Jürimäe, C. Lycourgos i N. Piçarra, suci,

nezavisni odvjetnik: M. Campos Sánchez-Bordona,

tajnik: C. Strömholm, administratorica,

uzimajući u obzir pisani postupak i nakon rasprave održane 9. i 10. rujna 2019.,

* Jezik postupka: engleski

uzimajući u obzir očitovanja koja su podnijeli:

– za Privacy International, B. Jaffey i T. de la Mare, *QC*, D. Cashman, *solicitor*, i H. Roy, *avocat*,

– za vladu Ujedinjene Kraljevine, Z. Lavery, D. Guðmundsdóttir i S. Brandon, u svojstvu agenata, uz asistenciju G. Facennea, D. Bearda, *QC*, C. Knighta i R. Palmera, *barristers*,

– za belgijsku vladu, P. Cottin i J.-C. Halleux, u svojstvu agenata, uz asistenciju J. Vanpraeta, *advocaat*, i E. de Lophema, *avocat*,

– za češku vladu, M. Smolek, J. Vláčil i O. Serdula, u svojstvu agenata,

– za njemačku vladu, M. Hellmann, R. Kanitz, D. Klebs i T. Henze, a zatim J. Möller, M. Hellmann, R. Kanitz i D. Klebs, u svojstvu agenata,

– za estonsku vladu, A. Kalbus, u svojstvu agenta,

– za irsku vladu, M. Browne, G. Hodge i A. Joyce, u svojstvu agenata, uz asistenciju D. Fennellyja, *barrister*,

– za španjolsku vladu, L. Aguilera Ruiz i M. J. García-Valdecasas Dorrego, a zatim L. Aguilera Ruiz, u svojstvu agenata,

– za francusku vladu, E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas i D. Dubois, a zatim E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune i D. Dubois, u svojstvu agenata,

– za ciparsku vladu, E. Symeonidou i E. Neofytou, u svojstvu agenata,

– za latvijsku vladu, V. Soņeca i I. Kucina, a zatim V. Soņeca, u svojstvu agenata,

– za mađarsku vladu, G. Koós, M. Z. Fehér, G. Tornyai i Z. Wagner, a zatim G. Koós i M. Z. Fehér, u svojstvu agenata,

– za nizozemsku vladu, C. S. Schillemans i M. K. Bulterman, u svojstvu agentica,

– za poljsku vladu, B. Majczyna, J. Sawicka i M. Pawlicka, u svojstvu agenata,

– za portugalsku vladu, L. Inez Fernandes, M. Figueiredo i F. Aragão Homem, u svojstvu agenata,

– za švedsku vladu, A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren i A. Alriksson, a zatim H. Shev, C. Meyer-Seitz, L. Zettergren i A. Alriksson, u svojstvu agentica,

– za norvešku vladu, T. B. Leming, M. Emberland i J. Vangsnes, u svojstvu agenata,

– za Europsku komisiju, H. Kranenborg, M. Wasmeier, D. Nardi i P. Costa de Oliveira, a zatim H. Kranenborg, M. Wasmeier i D. Nardi, u svojstvu agenata,

– za Europskog nadzornika za zaštitu podataka, T. Zerdick i A. Buchta, u svojstvu agenata,

saslušavši mišljenje nezavisnog odvjetnika na raspravi održanoj 15. siječnja 2020.,

donosi sljedeću

Presudu

1 Zahtjev za prethodnu odluku odnosi se na tumačenje članka 1. stavka 3. i članka 15. stavka 1. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. (SL 2009., L 337, str. 11.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 224. i ispravci SL 2017., L 162, str. 56. i SL 2018., L 74, str. 11.) (u daljnjem tekstu: Direktiva 2002/58), u vezi s člankom 4. stavkom 2. UEU-a kao i člancima 7. i 8. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja).

2 Zahtjev je upućen u okviru spora između Privacy Internationala, s jedne strane, i Secretary of State for Foreign and Commonwealth Affairs (ministar vanjskih poslova i poslova Commonwealtha, Ujedinjena Kraljevina), Secretary of State for the Home Departement (ministar unutarnjih poslova, Ujedinjena Kraljevina), Government Communications Headquarters (Vladin komunikacijski stožer, Ujedinjena Kraljevina) (u daljnjem tekstu: GCHQ), Security Service (Sigurnosna služba, Ujedinjena Kraljevina, u daljnjem tekstu: MI5) i Secret Intelligence Service (Tajna obavještajna služba, Ujedinjena Kraljevina; u daljnjem tekstu: MI6), s druge strane, u vezi sa zakonitošću propisa kojima se dopušta da sigurnosne i obavještajne službe prikupljaju i upotrebljavaju masovne komunikacijske podatke *(bulk communications data)*.

Pravni okvir

Pravo Unije

Direktiva 95/46

3 Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.) stavljena je izvan snage Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (SL 2016., L 119, str. 1. i ispravak SL 2018., L 127, str. 2.), s učinkom od 25. svibnja 2018. Članak 3. navedene direktive, naslovljen „Područje primjene”, glasi kako slijedi:

„1. Ova Direktiva se primjenjuje na osobne podatke koji se u cijelosti ili djelomično obrađuju automatskim putem i na obradu podataka koja nije automatska, a koja čini dio sustava arhiviranja ili će činiti dio sustava arhiviranja.

2. Ova se Direktiva ne primjenjuje na obradu osobnih podataka:

– tijekom aktivnosti koja je izvan područja primjene prava Zajednice, kao što je predviđeno u glavama V. i VI. [UEU-a] i u svakom slučaju na postupke obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se operacija obrade odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava,

– koju provodi fizička osoba tijekom aktivnosti isključivo osobne ili domaće naravi.”

Direktiva 2002/58

4 U uvodnim izjavama 2., 6., 7., 11., 22., 26. i 30. Direktive 2002/58 navodi se:

„(2) Ova Direktiva traži poštovanje temeljnih prava te poštuje načela priznata posebno [Poveljom]. Ova Direktiva posebno traži osiguranje punoga poštovanja prava određenih u člancima 7. i 8. [te Povelje].

[…]

(6) Internet mijenja tradicionalne tržišne strukture pružajući zajedničku globalnu infrastrukturu za dostavu širokog raspona elektroničkih komunikacijskih usluga. Javno dostupne elektroničke komunikacijske usluge preko interneta otvaraju korisnicima nove mogućnosti, ali također i nove opasnosti za njihove osobne podatke i privatnost.

(7) U slučaju javnih komunikacijskih mreža treba donijeti posebne zakone i druge propise s ciljem zaštite temeljnih prava i sloboda fizičkih osoba i legitimnih interesa pravnih osoba, posebno u vezi sa sve većom sposobnošću automatskog pohranjivanja i obrade podataka koji se odnose na pretplatnike i korisnike.

[…]

(11) Poput Direktive [95/46], ova Direktiva ne obuhvaća pitanja zaštite temeljnih prava i sloboda koje se odnose na aktivnosti koje nisu uređene pravom [Unije]. Stoga se njome ne mijenja postojeća ravnoteža između prava na privatnost pojedinca i mogućnosti država članica da poduzmu mjere iz članka 15. stavka 1. ove Direktive, koje su nužne za zaštitu javne sigurnosti, obrane, državne sigurnosti (uključujući gospodarsko blagostanje države kada se aktivnosti odnose na sigurnosna pitanja države) te za provođenje odredaba kaznenog prava. Kao posljedica toga, ova Direktiva ne utječe na sposobnost država članica da provode zakonito presretanje elektroničkih komunikacija, odnosno da poduzimaju druge mjere ako je to nužno u neku od gore navedenih svrha te u skladu s Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda, [potpisanom u Rimu 4. studenog 1950.,] na način kako je tumači Europski sud za ljudska prava. Takve mjere moraju biti prikladne, strogo razmjerne svrsi za koju se poduzimaju i neophodne unutar demokratskog društva te trebaju biti podložne prikladnim zaštitnim mehanizmima u skladu s Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda.

[…]

(22) Zabrana pohranjivanja komunikacija i s njima povezanih podataka o prometu osobama koje nisu korisnici ili bez pristanka korisnika, nema namjeru zabraniti automatsko, posredničko i privremeno pohranjivanje ovih informacija u onoj mjeri u kojoj se ono odvija isključivo u svrhu provedbe prijenosa u elektroničkoj komunikacijskoj mreži te pod uvjetom da te informacije nisu pohranjene na razdoblje koje je duže od razdoblja potrebnog za svrhe prijenosa i upravljanja prometom, kao i pod uvjetom da tijekom razdoblja pohrane povjerljivost ostane zajamčena. Ako je to potrebno kako bi prijenos bilo koje javno dostupne informacije drugim primateljima usluge na njihov zahtjev bio učinkovitiji, ova Direktiva ne bi trebala sprečavati daljnju pohranu takve informacije, pod uvjetom da ta informacija u svakom slučaju bude dostupna javnosti, bez ograničenja, te da se svi podaci koji se odnose na pojedine pretplatnike ili korisnike koji zahtijevaju takve informacije obrišu.

[…]

(26) Podaci o pretplatnicima obrađeni unutar elektroničkih komunikacijskih mreža u svrhu uspostavljanja veze i prijenosa informacija sadrže informacije o privatnom životu fizičkih osoba te se tiču prava na poštovanje njihove korespondencije, odnosno legitimnih interesa pravnih osoba. Takvi se podaci mogu pohraniti isključivo u onoj mjeri koja je nužna za pružanje usluge u svrhu zaračunavanja i naplate međusobnog povezivanja te na ograničeno vrijeme. Bilo kakva daljnja obrada takvih podataka […] može se dopustiti samo ako se pretplatnik složio s time na temelju točne i potpune informacije koju je dobio od davatelja javno dostupnih elektroničkih komunikacijskih usluga o vrstama daljnje obrade koju davatelj usluga namjerava provesti te o pravu pretplatnika da ne pruži, odnosno opozove svoj pristanak na takvu obradu. Podaci o prometu koji su se koristili za marketinške komunikacijske usluge […] također se trebaju brisati ili učiniti anonimnima […]

[…]

(30) Sustave pružanja elektroničkih komunikacijskih mreža i usluga treba koncipirati tako da ograniče količinu nužnih osobnih podataka na strogi minimum. […]”

5 Članak 1. Direktive 2002/58, naslovljen „Područje primjene i cilj”, određuje:

„1. Direktiva osigurava usklađenost nacionalnih odredbi koje su potrebne kako bi se osigurala odgovarajuća razina zaštite osnovnih prava i sloboda, a posebno prava na privatnost i povjerljivost, s obzirom na obradu osobnih podataka u području elektroničkih komunikacija, te kako bi se osiguralo slobodno kretanje takvih podataka i elektroničke komunikacijske opreme i usluga u [Europskoj uniji].

2. Odredbe ove Direktive pojašnjavaju i nadopunjuju Direktivu [95/46] u svrhe spomenute u stavku 1. Štoviše, one pružaju zaštitu legitimnih interesa pretplatnika koji su pravne osobe.

3. Ova se Direktiva ne primjenjuje na aktivnosti koje su izvan područja primjene [UFEU-a], poput onih obuhvaćenih glavama V. i VI. Ugovora o Europskoj uniji, te, u svakom slučaju, na aktivnosti koje se odnose na javnu sigurnost, obranu, državnu sigurnost (uključujući gospodarsku dobrobit države kada se aktivnosti odnose na pitanja državne sigurnosti) te na aktivnosti države u području kaznenog prava.”

6 U skladu s člankom 2. te direktive, naslovljenim „Definicije”:

„Definicije iz Direktive [95/46] i Direktive 2002/21/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva) [(SL 2002., L 108, str. 33.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 49., str. 25.)] primjenjuju se osim ako nije drukčije određeno.

Sljedeće definicije se također primjenjuju:

(a) ‚korisnik’ znači svaka fizička osoba koja koristi javno dostupnu elektroničku komunikacijsku uslugu, u privatne ili poslovne svrhe, pri čemu nije nužno da se pretplatila na tu uslugu;

(b) ‚podaci o prometu’ znači svi podaci koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje;

(c) ‚podaci o lokaciji’ znači svi podaci koji se obrađuju u sklopu elektroničke komunikacijske mreže ili u sklopu usluga elektroničkih komunikacija, koji ukazuju na zemljopisnu lokaciju terminalne opreme korisnika javno dostupnih usluga elektroničkih komunikacija;

(d) ‚komunikacija' znači svaka informacija koja se razmjenjuje ili prenosi između ograničenog broja stranaka putem javno dostupne elektroničke komunikacijske usluge. Ovo ne uključuje informaciju prenesenu kao dio usluge emitiranja za javnost putem elektroničke komunikacijske mreže, osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju koji se mogu identificirati;

[…]"

7 Članak 3. navedene direktive, naslovljen „Usluge", predviđa:

„Ova se Direktiva primjenjuje na obradu osobnih podataka vezanih uz pružanje javno dostupnih usluga elektroničkih komunikacija na javno dostupnim komunikacijskim mrežama u [Uniji], uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i naprava za identifikaciju."

8 U skladu s člankom 5. Direktive 2002/58, naslovljenim „Povjerljivost komunikacija":

„1. Države članice putem svojih zakonodavstava osiguravaju povjerljivost komunikacija i s time povezanih podataka o prometu koji se šalju preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga. One posebno zabranjuju svim osobama koje nisu korisnici slušanje, prisluškivanje, pohranjivanje ili druge oblike presretanja odnosno nadzora nad komunikacijama i s time povezanim podacima o prometu, bez pristanka korisnika, osim u slučaju kada imaju zakonsko dopuštenje da to učine u skladu s člankom 15. stavkom 1. Ovaj stavak ne sprečava tehničko pohranjivanje koje je nužno za prijenos komunikacije, ne dovodeći u pitanje načelo povjerljivosti.

[…]

3. Države članice osiguravaju da je pohranjivanje podataka ili uspostavljanje pristupa već pohranjenim podacima na terminalnoj opremi pretplatnika ili korisnika, dozvoljeno samo pod uvjetom da je dotični pretplatnik ili korisnik dao svoj pristanak, nakon što je iscrpno i razumljivo, u skladu s Direktivom [95/46], između ostalog obaviješten o namjeni postupka obrade. Navedeno ne sprečava nikakav oblik tehničke pohrane ili pristupa samo u svrhu izvršavanja prijenosa komunikacije putem elektroničke komunikacijske mreže ili ako je to strogo potrebno, kako bi operator usluge informacijskog društva mogao pružiti uslugu koju je izričito zatražio pretplatnik ili korisnik."

9 Članak 6. Direktive 2002/58, naslovljen „Podaci o prometu", određuje:

„1. Podaci o prometu koji se odnose na pretplatnike i korisnike i koje je davatelj javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge obradio i pohranio moraju se obrisati ili učiniti anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije, ne dovodeći u pitanje stavke 2., 3. i 5. ovog članka te članak 15. stavak 1.

2. Podaci o prometu koji su nužni u svrhu naplaćivanja usluge od pretplatnika te u svrhu plaćanja međusobnog povezivanja mogu se obraditi. Takva je obrada dopustiva isključivo do kraja razdoblja tijekom kojega se račun može pravno pobijati ili tijekom kojega se može zahtijevati plaćanje.

3. Za potrebe marketinga usluga elektroničkih komunikacijska ili za potrebe pružanja usluga s dodatnom vrijednošću, operator javno dostupnih usluga elektroničkih komunikacija može obraditi podatke iz stavka 1. u onoj mjeri te u onom vremenskom razdoblju koje je neophodno za takve usluge ili marketing, ako je pretplatnik ili korisnik na kojeg se odnose podaci prethodno dao svoj pristanak. Korisnicima ili pretplatnicima u svakome trenutku daje se mogućnost povlačenja njihovog odobrenja za obradu podataka o prometu.

[…]

5. Obrada podataka o prometu, u skladu sa stavcima 1., 2., 3. i 4. mora se ograničiti na osobe koje djeluju pod nadzorom davatelja javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga i koje se bave naplaćivanjem usluga ili upravljanjem prometom, upitima potrošača, otkrivanjem prijevara, marketingom elektroničkih komunikacijskih usluga ili pružanjem usluga s posebnom tarifom, te mora biti ograničena na ono što je nužno u svrhe takvih aktivnosti."

10 Članak 9. te direktive, naslovljen „Podaci o lokaciji koji nisu podaci o prometu" predviđa u svojem stavku 1.:

„Ako se mogu obraditi podaci o lokaciji koji nisu podaci o prometu, koji se odnose na korisnike ili pretplatnike javnih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga, takvi podaci mogu se obraditi samo nakon što su učinjeni anonimnima, odnosno uz pristanak korisnika ili pretplatnika, u mjeri i u trajanju potrebnom za pružanje usluge s dodatnom vrijednosti. Davatelj usluga mora obavijestiti korisnike ili pretplatnike, prije dobivanja njihovog pristanka, o vrsti podataka o lokaciji koji nisu podaci o prometu koji će se obraditi, o svrsi i trajanju obrade te hoće li se dotični podaci proslijediti trećoj osobi u svrhu pružanja usluge s posebnom tarifom. […]"

11 Člankom 15. stavkom 1. navedene direktive, naslovljenim „Primjena određenih odredaba Direktive [95/46]", propisano je:

„Države članice mogu donijeti zakonske mjere kojima će ograničiti opseg prava i obveza koji pružaju članak 5., članak 6., članak 8. stavci 1., 2., 3. i 4., te članak 9. ove Direktive kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti (odnosno državne sigurnosti), obrane, javne sigurnosti te s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava iz članka 13. stavka 1. Direktive [95/46]. S tim u vezi, države članice mogu, između ostalog, donijeti zakonske mjere kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja opravdane razlozima određenim u ovom stavku. Sve mjere iz ovog stavka moraju biti u skladu s općim načelima prava [Unije], uključujući ona iz članka 6. stavaka 1. i 2. Ugovora o Europskoj uniji."

Uredba 2016/679

12 Članak 2. Uredbe 2016/679 određuje:

„1. Ova se Uredba primjenjuje na obradu osobnih podataka koja se u cijelosti [ili djelomično] obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

2. Ova se Uredba ne odnosi na obradu osobnih podataka:

(a) tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije;

(b) koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a;

[…]

(d) koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.

[…]"

13 Članak 4. te uredbe predviđa:

„Za potrebe ove Uredbe:

[…]

2. ‚obrada' znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

[…]"

14 Sukladno članku 23. stavku 1. iste uredbe:

„Na temelju prava Unije ili prava države članice kojem podliježu voditelj obrade podataka ili izvršitelj obrade zakonskom mjerom može se ograničiti opseg obveza i prava iz članaka od 12. do 22. i članka 34. te članka 5. ako te odredbe odgovaraju pravima i obvezama predviđenima u člancima od 12. do 22., ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu:

(a) nacionalne sigurnosti,

(b) obrane;

(c) javne sigurnosti;

(d) sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

(e) drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, osobito važnog gospodarskog ili financijskog interesa Unije ili države članice, što uključuje monetarna, proračunska i porezna pitanja, javno zdravstvo i socijalnu sigurnost;

(f) zaštite neovisnosti pravosuđa i sudskih postupaka;

(g) sprečavanja, istrage, otkrivanja i progona kršenja etike za regulirane struke;

(h) funkcije praćenja, inspekcije ili regulatorne funkcije koja je, barem povremeno, povezana s izvršavanjem službene ovlasti u slučajevima iz točaka od (a) do (e) i točke (g);

(i) zaštite ispitanika ili prava i sloboda drugih.

(j) ostvarivanja potraživanja u građanskim sporovima."

15 U skladu s člankom 94. stavkom 2. Uredbe br. 2016/679:

„Upućivanja na direktivu koja je stavljena izvan snage tumače se kao upućivanja na ovu Uredbu. Upućivanja na Radnu skupinu o zaštiti pojedinaca s obzirom na obradu osobnih podataka osnovanu člankom 29. Direktive [95/46] tumače se kao upućivanja na Europski odbor za zaštitu podataka osnovan ovom Uredbom."

Pravo Ujedinjene Kraljevine

16 Članak 94. Telecommunications Acta 1984 (Zakon iz 1984. o telekomunikacijama), u verziji primjenjivoj na činjenice u glavnom postupku (u daljnjem tekstu: Zakon iz 1984.), naslovljen „Smjernice u interesu nacionalne sigurnosti itd.”, određuje:

„1. Nakon savjetovanja s osobom na koju se ovaj članak primjenjuje, ministar može toj osobi dati opće smjernice u mjeri u kojoj smatra da je to u interesu nacionalne sigurnosti ili odnosa s vladom zemlje ili područja koji se nalaze izvan Ujedinjene Kraljevine.

2. Ako ministar smatra nužnim postupiti tako u interesu nacionalne sigurnosti ili odnosa s vladom zemlje ili područja koji se nalaze izvan Ujedinjene Kraljevine, on može, nakon savjetovanja s osobom na koju se ovaj članak primjenjuje, dati toj osobi smjernice zahtijevajući od nje (ovisno o okolnostima slučaja) da obavi ili ne obavi određenu radnju navedenu u smjernicama.

2.A Ministar može dati smjernice na temelju stavka 1. ili 2. samo ako smatra da je postupanje koje je potrebno na osnovi smjernica proporcionalno cilju koji treba postići tim postupanjem.

3. Osoba na koju se ovaj članak primjenjuje mora provesti sve smjernice koje joj je ministar dao na temelju ovog članka, neovisno o bilo kojoj drugoj obvezi koju ima na temelju dijela 1. ili dijela 2. poglavlja 1. Communications Acta 2003 [Zakon o telekomunikacijama iz 2003.] te, u slučaju smjernica danih pružatelju javne elektroničke komunikacijske mreže, čak i ako se navedene smjernice primjenjuju na njega po osnovi svojstva različitog od svojstva pružatelja pristupa takvoj mreži.

4. U svakom od domova Parlamenta ministar pohranjuje presliku svih smjernica danih na temelju ovog članka, osim ako smatra da bi otkrivanje navedenih smjernica bilo suprotno interesima nacionalne sigurnosti ili odnosa s vladom zemlje ili područja koji se nalaze izvan Ujedinjene Kraljevine, ili poslovnim interesima određene osobe.

5. Nitko ne treba otkriti niti se od njega može zahtijevati da otkrije, na temelju zakona ili po drugoj osnovi, ikakve informacije u vezi s mjerama koje su donesene u skladu s ovim člankom, ako ga je ministar obavijestio da je prema njegovu mišljenju otkrivanje tih informacija suprotno interesima nacionalne sigurnosti ili odnosa s vladom zemlje ili područja koji se nalaze izvan Ujedinjene Kraljevine, ili poslovnim interesima druge osobe.

[…]

(8) Ovaj se članak primjenjuje na [Office of communications (Ured za komunikacije) (OFCOM)] i na pružatelje javnih elektroničkih komunikacijskih mreža.”

17 Članak 21. stavci 4. i 6. Regulation of Investigatory Powers Acta 2000 (Zakon iz 2000. o istražnim ovlastima, u daljnjem tekstu: RIPA) određuje:

„4. [I]zraz ‚podaci o komunikacijama’ znači bilo što od navedenog:

(a) bilo koji podatak o prometu sadržan u komunikaciji ili koji joj je priložen (od pošiljatelja ili na drugi način) u svrhu bilo koje poštanske usluge ili telekomunikacijskog sustava kojim se ti podaci prenose ili se mogu prenositi;

(b) bilo koja informacija koja ne uključuje ništa od sadržaja komunikacije (osim bilo koje informacije iz točke (a)) i koja se odnosi na korištenje bilo koje osobe:
   (i) bilo koje poštanske ili telekomunikacijske usluge; ili
   (ii) u vezi s pružanjem bilo koje telekomunikacijske usluge bilo kojeg dijela telekomunikacijskog sustava bilo kojoj osobi ili korištenje tom uslugom bilo koje osobe;

(c) bilo koja informacija koja nije obuhvaćena točkama (a) ili (b) koju je zadržala ili dobila u pogledu primatelja usluge osoba koja pruža poštansku ili telekomunikacijsku uslugu.

[…]

6. [P]ojam ‚podatak o prometu', u pogledu bilo koje komunikacije odnosi se na:

(a) bilo koji podatak kojim se utvrđuje ili može utvrditi bilo koja osoba, uređaj ili lokacija prema kojoj ili od koje se prenosi ili može prenijeti komunikacija;

(b) bilo koji podatak kojim se utvrđuje ili odabire, ili kojim se može utvrditi ili odabrati uređaj s pomoću kojeg se prenosi ili može prenijeti komunikacija;

(c) bilo koji podatak koji sadržava signale za pokretanje uređaja koji se upotrebljava za potrebe komunikacijskog sustava u svrhu prijenosa bilo kakve komunikacije; i

(d) bilo koji podatak kojim se utvrđuju podaci sadržani u posebnoj komunikaciji ili koji su joj priloženi ili drugi podaci dokle god su sadržani u posebnoj komunikaciji ili su joj priloženi.

[…]"

18 Članci 65. do 69. RIPA-e određuju pravila o funkcioniranju i nadležnostima Investigatory Powers Tribunala (Sud za istražne ovlasti, Ujedinjena Kraljevina). U skladu s člankom 65. tog zakona, pritužbe se tom sudu mogu podnijeti ako postoji razlog na temelju kojeg se može smatrati da su podaci dobiveni na neprimjeren način.

Glavni postupak i prethodna pitanja

19 Na početku 2015. postojanje praksi prikupljanja i upotrebe masovnih komunikacijskih podataka od strane različitih sigurnosnih i obavještajnih službi Ujedinjene Kraljevine, to jest GCHQ-a, MI5-a i MI6-a, učinjeno je javnim osobito u izvješću Intelligence and Security Committee of Parliament (odbor Parlamenta za obavještajne poslove i sigurnost, Ujedinjena Kraljevina). Dana 5. lipnja 2015., nevladina organizacija Privacy International pokrenula je pred Investigatory Powers Tribunalom (Sud za istražne ovlasti, Ujedinjena Kraljevina) postupak protiv ministra vanjskih poslova i poslova Commonwealtha, ministra unutarnjih poslova te tih sigurnosnih i obavještajnih službi, osporavajući zakonitost tih praksi.

20 Sud koji je uputio zahtjev ispitao je zakonitost navedenih praksi prvenstveno s obzirom na unutarnje pravo i odredbe Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda, potpisane u Rimu 4. studenog 1950., (u daljnjem tekstu: EKLJP), a potom i na pravo Unije. U presudi od 17. listopada 2016., taj je sud utvrdio da su tuženici u glavnom postupku priznali da u okviru svojih aktivnosti navedene sigurnosne i obavještajne službe prikupljaju i upotrebljavaju skupove podataka koji se tiču pojedinaca i spadaju u različite kategorije *(bulk personal data)*, poput biografskih podataka ili podataka o putovanjima, financijskih ili poslovnih informacija, podataka u vezi s komunikacijama koji mogu sadržavati osjetljive podatke obuhvaćene profesionalnom tajnom, ili pak novinarskog materijala. Ti podaci, koji su pribavljeni na različite načine, po potrebi i tajno, analizirani su unakrsnom provjerom i posredstvom automatske obrade, mogu se otkrivati drugim osobama i tijelima te dijeliti s inozemnim partnerima. U tom okviru sigurnosne i obavještajne službe upotrebljavaju također masovne komunikacijske podatke, koji su prikupljeni od pružatelja javnih elektroničkih komunikacijskih mreža, među ostalim na temelju ministarskih smjernica donesenih na osnovi članka 94. Zakona iz 1984. godine. GCHQ i MI5 su tako postupali od 2001. odnosno 2005.

21 Navedeni je sud smatrao da su te mjere prikupljanja i upotrebljavanja podataka u skladu s unutarnjim pravom te od 2015., ovisno o još neispitanim pitanjima u vezi s proporcionalnošću navedenih mjera i prijenosom podataka trećim stranama, s člankom 8. EKLJP-a. U tom potonjem pogledu on je pojasnio da su podneseni dokazi o primjenjivim jamstvima, osobito glede postupaka za pristup podacima i njihovo otkrivanje izvan sigurnosnih i obavještajnih službi, načina za zadržavanje podataka i postojanja neovisnog nadzora.

22 Glede zakonitosti mjera prikupljanja i uporabe o kojima je riječ u glavnom postupku s obzirom na pravo Unije, sud koji je uputio zahtjev ispitao je u presudi od 8. rujna 2017., spadaju li te mjere u područje primjene tog prava i, u slučaju potvrdnog odgovora, jesu li one spojive s tim pravom. Glede masovnih komunikacijskih podataka, taj je sud utvrdio da su pružatelji elektroničkih komunikacijskih mreža dužni, na temelju članka 94. Zakona iz 1984. i u slučaju smjernica u tom smislu koje potječu od ministra, dostaviti sigurnosnim i obavještajnim službama podatke prikupljene u okviru svoje gospodarske djelatnosti obuhvaćene pravom Unije. S druge strane, to nije bio slučaj za prikupljanje drugih podataka koje su te službe pribavile bez korištenja obvezujućih ovlasti. Na temelju tog utvrđenja, taj je sud smatrao nužnim obratiti se Sudu kako bi se utvrdilo je li sustav poput onog koji proizlazi iz tog članka 94. obuhvaćen pravom Unije, i u slučaju potvrdnog odgovora, primjenjuju li se na taj sustav i na koji način zahtjevi koji su postavljeni u sudskoj praksi koja proizlazi iz presude od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, u daljnjem tekstu: presuda Tele2, EU:C:2016:970).

23 U tom pogledu sud koji je uputio zahtjev navodi u svojem zahtjevu da prema članku 94. ministar može pružateljima elektroničkih komunikacijskih usluga dati opće ili posebne smjernice koje mu se čine nužnima u interesu nacionalne sigurnosti ili odnosa s inozemnom vladom. Upućujući na definicije u članku 21. stavcima 4. i 6. RIPA-e, taj sud pojašnjava da dotični podaci uključuju podatke o prometu kao i informacije o korištenim uslugama u smislu ove potonje odredbe, pri čemu je isključen samo sadržaj komunikacija. Ti podaci i informacije omogućuju, među ostalim, da se glede određene komunikacije sazna „tko, gdje, kada i kako”. Navedeni se podaci prenose sigurnosnim i obavještajnim službama i ove potonje ih zadržavaju za potrebe svojih aktivnosti.

24 Navedeni sud smatra da se sustav o kojemu je riječ u glavnom postupku razlikuje od onoga koji proizlazi iz Data Retention and Investigatory Powers Acta 2014 (Zakon iz 2014. o zadržavanju podataka i istražnim ovlastima), o kojemu je riječ u predmetu povodom kojeg je donesena presuda od 21. prosinca 2016., Tele2 (C-203/15 i C-698/15, EU:C:2016:970), jer je ovim potonjim sustavom predviđeno da pružatelji elektroničkih komunikacijskih usluga zadržavaju podatke i da ih se ne stavlja na raspolaganje samo sigurnosnim i obavještajnim službama u interesu nacionalne sigurnosti, nego i drugim javnim tijelima, ovisno o njihovim potrebama. Ta se presuda odnosila, osim toga, na kaznenu istragu, a ne na nacionalnu sigurnost.

25 Sud koji je uputio zahtjev dodaje da su baze podataka koje sastavljaju sigurnosne i obavještajne službe predmet masovne, a ne posebne, automatske obrade, kojom se nastoji otkriti postojanje mogućih eventualnih prijetnji. U tu svrhu taj sud navodi da svi metapodaci koji su tako prikupljeni trebaju biti što potpuniji kako bi se moglo raspolagati „plastom sijena” da se nađe „igla” koja je u njemu skrivena. U vezi s koristi od prikupljanja masovnih podataka od strane navedenih službi i tehnikama provjere tih podataka, navedeni sud upućuje osobito na zaključke iz izvješća koje je 19. kolovoza 2016. sastavio David Anderson, *QC*, tada United Kingdom Independent Reviewer of Terrorism Legislation (neovisni nadzornik Ujedinjene Kraljevine nad zakonodavstvom o terorizmu), koji se radi sastavljanja tog izvješća oslonio na ispitivanje koje je provela skupina obavještajnih stručnjaka i na svjedočenja agenata sigurnosnih i obavještajnih službi.

26 Sud koji je uputio zahtjev pojašnjava također da je prema stajalištu Privacy Internationala, sustav o kojem je riječ u glavnom postupku nezakonit s obzirom na pravo Unije, dok tuženici u glavnom postupku smatraju da obveza prijenosa podataka predviđena tim sustavom, pristup tim podacima kao i njihova uporaba ne spadaju u nadležnosti Unije, osobito u skladu s člankom 4. stavkom 2. UEU-a prema kojem nacionalna sigurnost ostaje isključiva odgovornost svake države članice.

27 U tom pogledu sud koji je uputio zahtjev smatra, na temelju presude od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346, t. 56. do 59.), koja se odnosi na prijenos PNR podataka *(Passenger Name Record)* u svrhu zaštite javne sigurnosti, da se za aktivnosti trgovačkih društava u okviru obrade i prijenosa podataka radi zaštite nacionalne sigurnosti ne čini da spadaju u područje primjene prava Unije. Ne bi trebalo ispitati je li predmetna aktivnost obrada podataka, nego samo je li po svojoj biti i učincima predmet takve aktivnosti održavanje temeljne državne funkcije u smislu članka 4. stavka 2. UEU-a posredstvom okvira koji su utvrdila javna tijela u vezi s javnom sigurnošću.

28 U slučaju da su mjere o kojima je riječ u glavnom postupku ipak obuhvaćene pravom Unije, sud koji je uputio zahtjev smatra da za zahtjeve u točkama 119. do 125. presude od 21. prosinca 2016., Tele2 (C-203/15 i C-698/15, EU:C:2016:970), proizlazi da su neprikladni u kontekstu nacionalne sigurnosti i mogu potkopati sposobnost sigurnosnih i obavještajnih službi da se nose s određenim prijetnjama nacionalnoj sigurnosti.

29 U tim je okolnostima Investigatory Powers Tribunal (Sud za istražne ovlasti) odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:

„U okolnostima u kojima:

a) su sposobnosti [sigurnosnih i obavještajnih službi] da koriste [masovne komunikacijske podatke] koji im se dostavljaju, bitne za zaštitu nacionalne sigurnosti Ujedinjene Kraljevine, uključujući područja borbe protiv terorizma, protuobavještajnih aktivnosti i suzbijanja širenja nuklearnog oružja;

b) temeljno obilježje uporabe [masovnih komunikacijskih podataka] od strane [sigurnosnih i obavještajnih službi] jest otkrivanje prethodno nepoznatih prijetnji za nacionalnu sigurnost uporabom neciljanih masovnih tehnika koje se temelje na objedinjavanju masovnih komunikacijskih podataka na jednom mjestu. Glavna korist jest brzo utvrđivanje i praćenje mete, kao i pružanje osnove za akciju u situaciji neposredne prijetnje;

c) pružatelj elektroničke komunikacijske mreže nije naknadno obvezan zadržati [masovne komunikacijske podatke] (dulje od razdoblja koje zahtijeva njegovo uobičajeno poslovanje), a koje zatim zadržava samo država ([sigurnosne i obavještajne službe]);

d) je nacionalni sud utvrdio (ovisno o određenim pitanjima o kojima još nije odlučeno) da su zaštitne mjere u vezi s uporabom [masovnih komunikacijskih podataka] od strane [sigurnosnih i obavještajnih službi] dosljedne zahtjevima EKLJP-a; te

e) je nacionalni sud utvrdio da bi nalaganje zahtjeva navedenih u točkama 119.-125. presude [od 21. prosinca 2016., Tele2 (C-203/15 i C-698/15, EU:C:2016:970)], ako je primjenjivo, onemogućilo mjere sigurnosnih i obavještajnih službi poduzete radi zaštite nacionalne sigurnosti i stoga dovelo u opasnost nacionalnu sigurnost Ujedinjene Kraljevine;

1. Uzimajući u obzir članak 4. UEU-a i članak 1. stavak 3. Direktive [2002/58], obuhvaća li opseg prava Unije i Direktive [2002/58] zahtjev propisan smjernicom ministra kojim se pružatelju elektroničke komunikacijske mreže nalaže da sigurnosnim i obavještajnim službama države članice pruža masovne komunikacijske podatke?

2. Ako je odgovor na prvo pitanje potvrdan, primjenjuju li se na takvu smjernicu ministra neki od zahtjeva [primjenjivih na zadržane komunikacijske podatke navedene u točkama 119. do 125. presude od 21. prosinca 2016., Tele2 (C-203/15 i C-698/15, EU:C:2016:970)] odnosno i neki drugi zahtjevi uz one koji su propisani EKLJP-om? Ako je tomu tako, na koji se način i u kojoj mjeri ti zahtjevi primjenjuju, uzimajući u obzir bitnu potrebu [sigurnosnih i obavještajnih službi] da za zaštitu nacionalne sigurnosti koriste masovno prikupljanje i tehnike automatske obrade, te u kojoj mjeri propisivanje takvih zahtjeva može kritično onemogućiti takve sposobnosti, ako su one u drugim pogledima usklađene s EKLJP-om?"

Prethodna pitanja

Prvo pitanje

30 Svojim prvim pitanjem sud koji je uputio zahtjev pita, u biti, treba li članak 1. stavak 3. Direktive 2002/58, u vezi s člankom 4. stavkom 2. UEU-a, tumačiti na način da je područjem primjene te direktive obuhvaćen nacionalni propis koji državnom tijelu omogućuje da nalaže pružateljima elektroničkih komunikacijskih usluga da radi zaštite nacionalne sigurnosti prenose sigurnosnim i obavještajnim službama podatke o prometu i lokaciji.

31 U tom pogledu Privacy International navodi, u osnovi, da su s obzirom na upute iz sudske prakse Suda glede područja primjene Direktive 2002/58, kako prikupljanje podataka od strane sigurnosnih i obavještajnih službi od tih pružatelja na temelju članka 94. Zakona iz 1984. tako i njihova uporaba od strane navedenih službi obuhvaćeni područjem primjene te direktive, bez obzira na to jesu li navedeni podaci prikupljeni prijenosnom koji je obavljen izvan stvarnog vremena ili u stvarnom vremenu. Konkretno, činjenica da je cilj zaštite nacionalne sigurnosti izričito naveden u članku 15. stavku 1. navedene direktive nema za posljedicu neprimjenjivost ove potonje na takve situacije, a članak 4. stavak 2. UEU-a ne utječe na tu ocjenu.

32 S druge strane, vlada Ujedinjene Kraljevine, češka i estonska vlada, Irska kao i francuska, ciparska, mađarska, poljska i švedska vlada ističu, u biti, da se Direktiva 2002/58 ne primjenjuje na nacionalne propise o kojima je riječ u glavnom postupku, s obzirom na to da je njihova svrha zaštita nacionalne sigurnosti. Aktivnosti sigurnosnih i obavještajnih službi spadaju u temeljne funkcije država članica koje se odnose na održavanje javnog reda kao i zaštitu unutarnje sigurnosti i teritorijalne cjelovitosti te su, slijedom toga, u isključivoj nadležnosti ovih potonjih, kao što to dokazuje osobito članak 4. stavak 2. treća rečenica UEU-a.

33 Te vlade smatraju da se Direktiva 2002/58 ne može stoga tumačiti na način da nacionalne mjere namijenjene zaštiti nacionalne sigurnosti spadaju u njezino područje primjene. Članak 1. stavak 3. te direktive razgraničava to područje primjene te iz njega isključuje, poput onog što je već bilo predviđeno člankom 3. stavkom 2. prvom alinejom Direktive 95/46, aktivnosti u vezi s javnom sigurnošću, obranom i državnom sigurnošću. Te odredbe održavaju raspodjelu nadležnosti predviđenu u članku 4. stavku 2. te bi one bile lišene korisnog učinka, ako bi mjere koje spadaju u područje nacionalne sigurnosti morale poštovati zahtjeve iz Direktive 2002/58. Osim toga, sudska praksa Suda koja je proizašla iz presude od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346), koja se odnosi na članak 3. stavak 2. treću alineju Direktive 95/46, može se primijeniti na članak 1. stavak 3. Direktive 2002/58.

34 U tom pogledu valja navesti da na temelju svojeg članka 1. stavka 1., Direktiva 2002/58 predviđa, među ostalim, usklađenost nacionalnih odredaba koje su potrebne kako bi se osigurala odgovarajuća razina zaštite osnovnih prava i sloboda, a posebno prava na privatnost i povjerljivost, s obzirom na obradu osobnih podataka u području elektroničkih komunikacija.

35 Člankom 1. stavkom 3. te direktive iz njezina su područja primjene isključene „aktivnosti države” u područjima navedenima u tom članku, među ostalim, aktivnosti države u području kaznenog prava i aktivnosti koje se odnose na javnu sigurnost, obranu i državnu sigurnost, uključujući gospodarsku dobrobit države kada se aktivnosti odnose na pitanja državne sigurnosti. Aktivnosti koje su u tom članku navedene kao primjer u svakom su slučaju aktivnosti država odnosno državnih tijela koje ne ulaze u područje aktivnosti pojedinaca (presuda od 2. listopada 2018., Ministerio Fiscal, C-207/16, EU:C:2018:788, t. 32. i navedena sudska praksa).

36 Nadalje, člankom 3. Direktive 2002/58 određeno je da se ona primjenjuje na obradu osobnih podataka vezanih uz pružanje javno dostupnih usluga elektroničkih komunikacija na javno dostupnim komunikacijskim mrežama u Uniji, uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i naprava za identifikaciju (u daljnjem tekstu: elektroničke komunikacijske usluge). Slijedom toga, valja smatrati da se tom direktivom uređuju aktivnosti pružatelja takvih usluga (presuda od 2. listopada 2018., Ministerio Fiscal, C-207/16, EU:C:2018:788, t. 33. i navedena sudska praksa).

37 U tom okviru, članak 15. stavak 1. Direktive 2002/58 ovlašćuje države članice da donesu, uz poštovanje njome predviđenih uvjeta, „zakonske mjere kojima će ograničiti opseg prava i obveza koji pružaju članak 5., članak 6., članak 8. stavci 1., 2., 3. i 4., te članak 9. [te] direktive” (presuda od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 71.).

38 Naime, članak 15. stavak 1. Direktive 2002/58 nužno pretpostavlja da njime predviđene nacionalne zakonske mjere ulaze u područje primjene te direktive, s obzirom na to da se države članice njome izričito ovlašćuju na njihovo donošenje samo uz poštovanje njome predviđenih uvjeta. Usto, takvim se mjerama uređuju, u svrhe spomenute u toj odredbi, aktivnosti pružatelja usluga elektroničkih komunikacija (presuda od 2. listopada 2018., Ministerio Fiscal, C-207/16, EU:C:2018:788, t. 34. i navedena sudska praksa).

39 Osobito je s obzirom na ta razmatranja Sud presudio da članak 15. stavak 1. Direktive 2002/58, u vezi s njezinim člankom 3., treba tumačiti na način da u područje primjene te direktive ne ulazi samo zakonska mjera koja pružateljima usluga elektroničkih komunikacija nalaže zadržavanje podataka o prometu i lokaciji, nego i zakonska mjera kojom im se nalaže da nacionalnim nadležnim tijelima odobre pristup tim podacima. Naime, takve zakonske mjere nužno podrazumijevaju da navedeni pružatelji obrađuju navedene podatke i s obzirom na to da se navedenim mjerama uređuju aktivnosti tih istih pružatelja, one se ne mogu izjednačiti s aktivnostima država, o kojima je riječ u članku 1. stavku 3. navedene direktive (vidjeti u tom smislu presudu od 2. listopada 2018., Ministerio Fiscal, C-207/16, EU:C:2018:788, t. 35. i 37. i navedenu sudsku praksu).

40 Glede zakonske mjere poput članka 94. Zakona iz 1984., na temelju kojeg nadležno tijelo može pružateljima elektroničkih komunikacijskih usluga dati smjernicu da masovne podatke prijenosom dostavlja sigurnosnim i obavještajnim službama, valja istaknuti da na temelju definicije u članku 4. stavku 2. Uredbe 2016/679, koja je primjenjiva u skladu s člankom 2. Direktive 2002/58, u vezi s člankom 94. stavkom 2. navedene uredbe, pojam „obrada osobnih podataka” označava „svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, […] pohrana, […] obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način […]”.

41 Proizlazi da otkrivanje osobnih podataka prijenosom, isto kao i pohrana podataka ili stavljanje na raspolaganje na drugi način, jest obrada u smislu članka 3. Direktive 2002/58 i, slijedom toga, ulazi u područje primjene te direktive (vidjeti u tom smislu presudu od 29. siječnja 2008., Promusicae, C-275/06, EU:C:2008:54, t. 45.).

42 Nadalje, s obzirom na razmatranja u točki 38. ove presude i opću strukturu Direktive 2002/58, tumačenje te direktive, prema kojemu su zakonske mjere iz njezina članka 15. stavka 1. isključene iz područja primjene navedene direktive, jer se ciljevi kojima takve mjere moraju težiti u biti preklapaju s ciljevima aktivnosti iz članka 1. stavka 3. iste direktive, lišilo bi taj članak 15. stavak 1. bilo kakvog korisnog učinka (vidjeti u tom smislu presudu od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 72. i 73.).

43 Pojam „aktivnosti" u članku 1. stavku 3. Direktive 2002/58 ne može se dakle, kao što je to u osnovi istaknuo nezavisni odvjetnik u točki 75. svojeg mišljenja u spojenim predmetima La Quadrature du Net i dr. (C-511/18 i C-512/18, EU:C:2020:6), na koje on upućuje u točki 24. svojeg mišljenja u ovom predmetu, tumačiti na način da obuhvaća zakonske mjere iz članka 15. stavka 1. te direktive.

44 Odredbe članka 4. stavka 2. UEU-a, na koje upućuju vlade spomenute u točkama 32. ove presude, ne mogu oboriti taj zaključak. Naime, u skladu s ustaljenom sudskom praksom Suda, iako je na državama članicama da definiraju svoje osnovne interese sigurnosti i donesu prikladne mjere da osiguraju svoju unutarnju i vanjsku sigurnost, sama činjenica da je nacionalna mjera donesena radi zaštite nacionalne sigurnosti ne može dovesti do neprimjenjivosti prava Unije i osloboditi države članice obveze da nužno poštuju to pravo (vidjeti u tom smislu presude od 4. lipnja 2013., ZZ, C-300/11, EU:C:2013:363, t. 38. i navedenu sudsku praksu, od 20. ožujka 2018., Komisija/Austrija (Državna tiskara), C-187/16, EU:C:2018:194, t. 75. i 76., i od 2. travnja 2020., Komisija/Poljska, Mađarska i Češka Republika (Privremeni mehanizam za premještanje podnositelja zahtjeva za međunarodnu zaštitu), C-715/17, C-718/17 i C-719/17, EU:C:2020:257, t. 143. i 170.).

45 Točno je da je u presudi od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346, t. 56. do 59.) Sud presudio da prijenos osobnih podataka od strane zračnih prijevoznika javnim tijelima treće države u svrhu sprečavanja i borbe protiv terorizma i drugih teških kaznenih djela, nije na temelju članka 3. stavka 2. prve alineje Direktive 95/46 obuhvaćen područjem primjene te direktive, jer takav prijenos spada u okvir koji su uvela tijela javne vlasti i čiji je cilj zaštita javne sigurnosti.

46 Međutim, s obzirom na razmatranja u točkama 36., 38. i 39. ove presude, ta se sudska praksa ne može primijeniti prilikom tumačenja članka 1. stavka 3. Direktive 2002/58. Naime, kao što je to u osnovi istaknuo nezavisni odvjetnik u točkama 70. do 72. svojeg mišljenja u spojenim predmetima La Quadrature du Net i dr. (C-511/18 i C-512/18, EU:C:2020:6), članak 3. stavak 2. prva alineja Direktive 95/46, na koju se navedena sudska praksa odnosi, općenito je iz područja primjene ove potonje direktive isključivala „postupke obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost", te se njome nisu razlikovale osobe koje su obavljale dotičnu obradu podataka. S druge strane, u okviru tumačenja članka 1. stavka 3. Direktive 2002/58 takva se razlika pokazuje nužnom. Naime, kao što proizlazi iz točaka 37. do 39. i 42. ove presude, svi postupci obrade osobnih podataka koje provode pružatelji elektroničkih komunikacijskih usluga obuhvaćeni su područjem primjene navedene direktive, uključujući postupke obrade koji proizlaze iz obveza koje su im nametnula tijela javne vlasti, dok su ovi potonji postupci obrade mogli, ovisno o okolnostima, ući u područje primjene iznimke predviđene u članku 3. stavku 2. prvoj alineji Direktive 95/46 vodeći računa o široj formulaciji te odredbe koja obuhvaća sve postupke obrade čiji je cilj javna sigurnost, obrana ili nacionalna sigurnost, neovisno o osobi koja obavlja te aktivnosti.

47 Osim toga, valja istaknuti da je Direktiva 95/46, o kojoj je riječ u predmetu povodom koje je donesena presuda od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346), bila stavljena izvan snage na temelju članka 94. stavka 1. Uredbe 2016/679 te zamijenjena ovom potonjom, s učinkom od 25. svibnja 2018. No, iako je u članku 2. stavku 2. točki (d) navedene uredbe pojašnjeno da se ne primjenjuje na obrade koje obavljaju „nadležna tijela" u svrhu, među ostalim, sprečavanja i otkrivanja kaznenih djela, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja, iz članka 23. stavka 1. točaka (d) i (h) iste uredbe proizlazi da obrade osobnih podataka koje u te iste

svrhe obavljaju pojedinci spadaju u njezino područje primjene. Proizlazi da tumačenje članka 1. stavka 3., članka 3. i članka 15. stavka 1. Direktive 2002/58, koje prethodi, jest dosljedno razgraničenju područja primjene Uredbe 2016/679 koju ta direktiva dopunjuje i pojašnjava.

48 S druge strane, kada države članice izravno provode mjere koje odstupaju od povjerljivosti elektroničkih komunikacija, a da ne određuju obveze obrade pružateljima usluga takvih komunikacija, zaštita podataka dotičnih osoba nije obuhvaćena Direktivom 2002/58, nego samo nacionalnim pravom, podložno primjeni Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89.), tako da predmetne mjere moraju poštovati, među ostalim, nacionalno ustavno pravo i zahtjeve EKLJP-a.

49 S obzirom na prethodna razmatranja, na prvo pitanje treba odgovoriti da članak 1. stavak 3., članak 3. i članak 15. stavak 1. Direktive 2002/58, u vezi s člankom 4. stavkom 2. UEU-a, treba tumačiti na način da je područjem primjene te direktive obuhvaćen nacionalni propis koji državnom tijelu omogućuje da nalaže pružateljima elektroničkih komunikacijskih usluga da radi zaštite nacionalne sigurnosti prenose sigurnosnim i obavještajnim službama podatke o prometu i lokaciji.

Drugo pitanje

50 Svojim drugim pitanjem, sud koji je uputio zahtjev nastoji u biti saznati treba li članak 15. stavak 1. Direktive 2002/58, u vezi s člankom 4. stavkom 2. UEU-a, kao i člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje tumačiti na način da mu se protivi nacionalni propis koji državnom tijelu dopušta da radi zaštite nacionalne sigurnosti nalaže pružateljima elektroničkih komunikacijskih usluga da općenito i neselektivno prenose sigurnosnim i obavještajnim službama podatke o prometu i lokaciji.

51 Uvodno valja podsjetiti da prema navodima u zahtjevu za prethodnu odluku članak 94. Zakona iz 1984. ovlašćuje ministra da pružateljima elektroničkih komunikacijskih usluga naloži na temelju smjernica, kada to smatra nužnim u interesu nacionalne sigurnosti ili odnosa s inozemnom vladom, da sigurnosnim i obavještajnim službama prenose masovne komunikacijske podatke, pri čemu ti podaci uključuju podatke o prometu i lokaciji kao i informacije o korištenim uslugama, u smislu članka 21. stavaka 4. i 6. RIPA-e. Ova potonja odredba obuhvaća, osim toga, podatke nužne za identificiranje izvora komunikacije i njezina odredišta, određivanje datuma, vremena, trajanja i vrste komunikacije, identificiranje upotrijebljenog materijala kao i otkrivanje lokacije terminalne opreme i komunikacija, među kojim podacima se nalaze, *inter alia*, ime i adresa korisnika, telefonski broj pozivatelja i broj nazvane osobe, IP adrese izvora i adresata komunikacije kao i adrese posjećenih internetskih stranica.

52 Takva komunikacija prijenosnom podataka tiče se svih korisnika elektroničkih komunikacijskih sredstava, pri čemu nije pojašnjeno treba li do tog prijenosa doći u stvarnom vremenu ili naknadno. Prema navodima u zahtjevu za prethodnu odluku, jednom kada su preneseni, te podatke zadržavaju sigurnosne i obavještajne službe te ostaju na raspolaganju ovim potonjima za potrebe njihovih aktivnosti, kao i druge baze podataka koje te službe posjeduju. Konkretno, tako prikupljeni podaci, koji se podvrgavaju masovnim i automatiziranim obradama i analizama, mogu se unakrsno provjeriti s drugim bazama podataka koje sadržavaju različite kategorije masovnih osobnih podataka ili otkriti izvan tih službi i trećim državama. Naposljetku, ti postupci ne podliježu prethodnom odobrenju suda ili neovisnog upravnog tijela i ne dovode do ikakvog obavještavanja dotičnih osoba.

53 Direktiva 2002/58 ima za cilj, kao što to proizlazi među ostalim iz njezinih uvodnih izjava 6. i 7., zaštititi korisnike elektroničkih komunikacijskih usluga od opasnosti za njihove osobne podatke i njihov privatni život koje su rezultat novih tehnologija i osobito veće sposobnosti automatskog pohranjivanja i obrade podataka. Konkretno, navedena direktiva traži, kao što to proizlazi iz njezine

uvodne izjave 2., poštovanje prava utvrđenih u člancima 7. i 8. Povelje. U tom pogledu, iz obrazloženja prijedloga Direktive Europskog parlamenta i Vijeća o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (COM (2000) 385 *final*), na temelju kojeg je donesena Direktiva 2002/58, proizlazi da je zakonodavac Unije želio „postići to da visoka razina zaštite osobnih podataka i privatnog života bude i dalje zajamčena za sve elektroničke komunikacijske usluge, bez obzira na primijenjenu tehnologiju".

54 U tu svrhu članak 5. stavak 1. Direktive 2002/58 određuje da „[d]ržave članice putem svojih zakonodavstava osiguravaju povjerljivost komunikacija i s time povezanih podataka o prometu koji se šalju preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga". U toj se istoj odredbi naglašava također da „[države članice] posebno zabranjuju svim osobama koje nisu korisnici slušanje, prisluškivanje, pohranjivanje ili druge oblike presretanja odnosno nadzora nad komunikacijama i s time povezanim podacima o prometu, bez pristanka korisnika, osim u slučaju kada imaju zakonsko dopuštenje da to učine u skladu s člankom 15. stavkom 1." i pojašnjava da „[taj] stavak ne sprečava tehničko pohranjivanje koje je nužno za prijenos komunikacije, ne dovodeći u pitanje načelo povjerljivosti".

55 Stoga je u tom članku 5. stavku 1. utvrđeno načelo povjerljivosti kako elektroničkih komunikacija tako i s time povezanih podataka o prometu te podrazumijeva, među ostalim, načelnu zabranu svim osobama koje nisu korisnici da bez pristanka potonjih pohranjuju te komunikacije i te podatke. S obzirom na općenitost svojeg teksta, ta odredba nužno obuhvaća svaki postupak koji trećim osobama omogućuje da se upoznaju s komunikacijama i s time povezanim podacima u svrhe različite od prijenosa komunikacija.

56 Zabrana presretanja komunikacija i s time povezanih podataka u članku 5. stavku 1. Direktive 2002/58 obuhvaća, dakle, svaki oblik stavljanja javnim tijelima, poput sigurnosnih i obavještajnih službi, na raspolaganje podataka o prometu i lokaciji od strane pružatelja elektroničkih komunikacijskih usluga, kao i zadržavanje navedenih podataka od strane tih tijela, bez obzira na način na koji se oni kasnije upotrebljavaju.

57 Stoga je zakonodavac Unije, donijevši tu direktivu, konkretizirao prava utvrđena u člancima 7. i 8. Povelje, tako da uslijed izostanka vlastitog pristanka korisnici elektroničkih komunikacijskih sredstava imaju u načelu pravo očekivati da njihove komunikacije i s time povezani podaci ostanu anonimni i da se ne mogu bilježiti (presuda od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 109.).

58 Međutim, članak 15. stavak 1. Direktive 2002/58 dopušta državama članicama da uvedu iznimke od načelne obveze utvrđene u članku 5. stavku 1. te direktive, u vidu jamčenja povjerljivosti osobnih podataka kao i od odgovarajućih obveza spomenutih osobito u člancima 6. i 9. navedene direktive, kada je takvo ograničenje nužna, prikladna i proporcionalna mjera unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti, obrane i javne sigurnosti te s ciljem sprečavanja, istrage, otkrivanja ili progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava. S tim u vezi, države članice mogu, između ostalog, donijeti zakonske mjere kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja opravdane jednim od tih razloga.

59 S obzirom na to, mogućnost odstupanja od prava i obveza predviđenih u člancima 5., 6. i 9. Direktive 2002/58 ne može opravdati to da odstupanje od načelne obveze da se zajamči povjerljivost elektroničkih komunikacija i s time povezanih podataka, a osobito od zabrane pohrane tih podataka, koja je izričito predviđena u članku 5. te direktive, postane pravilo (vidjeti u tom smislu presude od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 89. i 104., i od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 111.).

60 Usto, iz članka 15. stavka 1. treće rečenice Direktive 2002/58 proizlazi da su zakonske mjere kojima će ograničiti opseg prava i obveza iz članaka 5., 6. i 9. te direktive države članice ovlaštene donositi samo u skladu s općim načelima prava Unije, među kojima se nalazi načelo proporcionalnosti, i temeljnim pravima koja su zajamčena Poveljom. U tom je pogledu Sud već presudio da obveza koju je nacionalnim propisom država članica odredila pružateljima elektroničkih komunikacijskih usluga da zadržavaju podatke o prometu kako bi se, u slučaju potrebe, ti podaci učinili dostupnima nadležnim nacionalnim tijelima, postavlja pitanja ne samo u vezi s poštovanjem članaka 7. i 8. Povelje, koji se odnose na zaštitu privatnog života i zaštitu osobnih podataka, nego i u vezi s člankom 11. Povelje koji se odnosi na slobodu izražavanja (vidjeti u tom smislu presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 25. i 70., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 91. i 92. i navedenu sudsku praksu).

61 Ta se ista pitanja postavljaju i za druge vrste obrade podataka, poput njihova prijenosa osobama različitim od korisnika ili pristupa tim podacima radi njihova korištenja (vidjeti po analogiji mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 122. i 123. i navedenu sudsku praksu).

62 Tako se prilikom tumačenja članka 15. stavka 1. Direktive 2002/58 treba uzeti u obzir važnost kako prava na poštovanje privatnosti zajamčenog člankom 7. Povelje tako i prava na zaštitu osobnih podataka zajamčenog njezinim člankom 8., kako proizlazi iz sudske prakse Suda, kao i prava na slobodu izražavanja, pri čemu je to temeljno pravo, zajamčeno u članku 11. Povelje, jedan od osnovnih temelja demokratskog i pluralističkog društva te je dio vrijednosti na kojima, u skladu s člankom 2. UEU-a, počiva Unija (vidjeti u tom smislu presude od 6. ožujka 2001., Connolly/Komisija, C-274/99 P, EU:C:2001:127, t. 39., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 93. i navedenu sudsku praksu).

63 Međutim, prava priznata člancima 7., 8. i 11. Povelje nisu apsolutna prava, nego ih treba uzeti u obzir imajući na umu njihovu funkciju u društvu (vidjeti u tom smislu presudu od 16. srpnja 2020., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, t. 172. i navedenu sudsku praksu).

64 Naime, kao što proizlazi iz članka 52. stavka 1. Povelje, ona priznaje ograničenja pri ostvarivanju tih prava samo ako su ograničenja predviđena zakonom, poštuju bit tih prava te su, uz poštovanje načela proporcionalnosti, nužna i zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

65 Valja dodati da uvjet da svako ograničenje ostvarivanja temeljnih prava mora biti predviđeno zakonom znači da se u samoj pravnoj osnovi kojom se dopušta zadiranje u ta prava mora definirati doseg ograničenja ostvarivanja dotičnog prava (presuda od 16. srpnja 2020., Facebook Ireland i Schrems, C-311/18, EU:C:2020:559, t. 175. i navedena sudska praksa).

66 Glede poštovanja načela proporcionalnosti, članak 15. stavak 1. prva rečenica Direktive 2002/58 određuje da države članice mogu donijeti mjeru koja odstupa od načela povjerljivosti komunikacija i s time povezanih podataka o prometu, kada je takva mjera „nužna, prikladna i proporcionalna unutar demokratskog društva” s obzirom na ciljeve koji su utvrđeni u toj odredbi. U uvodnoj izjavi 11. te direktive pojašnjeno je da takva mjera mora biti „strogo” proporcionalna svrsi za koju se poduzima.

67 U tom pogledu valja podsjetiti da zaštita temeljnog prava na poštovanje privatnog života zahtijeva, sukladno ustaljenoj sudskoj praksi Suda, da su odstupanja i ograničenja u zaštiti osobnih podataka u granicama onoga što je strogo nužno. Usto, cilj od općeg interesa ne može se postići, a da se u obzir ne uzme činjenica da se on mora pomiriti s temeljnim pravima na koje se mjera odnosi, tako da se cilj od općeg interesa pravilno odvagne s predmetnim pravima (vidjeti u tom smislu presude od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, t. 56., od

9. studenog 2010., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, t. 76., 77. i 86., i od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 52.; mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 140.).

68 Da bi ispunio uvjet proporcionalnosti, propis mora imati propisana jasna i precizna pravila kojima se uređuje doseg i primjena dotične mjere te propisivati minimalne uvjete, na način da osobe o čijim je osobnim podacima riječ raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu tih podataka od rizika zlouporabe. On mora biti zakonski obvezujuć u unutarnjem pravu i osobito navoditi u kojim se okolnostima i pod kojim uvjetima mjera kojom se predviđa obrada takvih podataka može donijeti, jamčeći time da će njezino zadiranje biti ograničeno na ono što je strogo nužno. Nužnost raspolaganja takvim jamstvima još je i značajnija kad su osobni podaci podvrgnuti automatskoj obradi, osobito kada postoji značajan rizik od nezakonitog pristupa tim podacima. Ti zaključci posebice vrijede kad je u pitanju zaštita jedne konkretne kategorije osobnih podataka, a to su osjetljivi podaci (vidjeti u tom smislu presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 54. i 55., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 117.; mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 141.).

69 Glede pitanja ispunjava li nacionalni propis, poput onoga o kojem je riječ u glavnom postupku, uvjete iz članka 15. stavka 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. kao i člankom 52. stavkom 1. Povelje, valja istaknuti da prijenos podataka o prometu i lokaciji osobama različitim od korisnika, poput sigurnosnih i obavještajnih službi, odstupa od načela povjerljivosti. Stoga kada se taj postupak provodi, kao u konkretnom slučaju, općenito i neselektivno, njime se od odstupanja od načelne obveze da se zajamči povjerljivost podataka stvara pravilo, iako sustav uspostavljen Direktivom 2002/58 zahtijeva da takvo odstupanje ostane iznimka.

70 Usto, u skladu s ustaljenom sudskom praksom Suda, prijenos podataka o prometu i lokaciji trećim osobama predstavlja zadiranje u temeljna prava predviđena člancima 7. i 8. Povelje, neovisno o kasnijem korištenju tim podacima. U tom je pogledu nevažno imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti (vidjeti u tom smislu mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 124. i 126. i navedenu sudsku praksu, i presudu od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 115. i 116.).

71 Miješanje prijenosa podataka o prometu i lokaciji sigurnosnim i obavještajnim službama u pravo utvrđeno člankom 7. Povelje treba smatrati osobito ozbiljnim, uzimajući u obzir, među ostalim, osjetljivost informacija koje mogu pružiti te podatke, a osobito mogućnost da se na temelju njih utvrdi profil predmetnih osoba, što je jednako osjetljiva informacija kao i sam sadržaj komunikacija. Ono usto može kod predmetnih osoba stvoriti osjećaj da je njihov privatni život predmet trajnog nadzora (vidjeti po analogiji presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 27. i 37., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 99. i 100.).

72 Valja još istaknuti da prijenos podataka o prometu i lokaciji javnim tijelima u sigurnosne svrhe može sam po sebi dovesti do ugrožavanja prava na poštovanje komunikacija utvrđenog u članku 7. Povelje i stvoriti odvraćajuće učinke na korisnike elektroničkih komunikacijskih sredstava da se koriste svojom slobodom izražavanja zajamčenom člankom 11. Povelje. Takvi odvraćajući učinci mogu osobito utjecati na osobe čije komunikacije podliježu, na temelju nacionalnih pravila, profesionalnoj tajni kao i na zviždače čije su aktivnosti zaštićene Direktivom (EU) 2019/1937 Europskog parlamenta i Vijeća od 23. listopada 2019. o zaštiti osoba koje prijavljuju povrede prava Unije (SL 2019., L 305, str. 17.). Usto, ti su učinci tim ozbiljniji što su broj i raznolikost zadržanih podataka veći (vidjeti u tom smislu presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 28.; od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 101., i od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 118.).

73 Naposljetku, vodeći računa o velikoj količini podataka o prometu i lokaciji koji se mogu kontinuirano zadržavati na temelju opće mjere zadržavanja kao i o osjetljivosti informacija koje mogu pružiti ti podaci, samo zadržavanje navedenih podataka od strane pružatelja elektroničkih komunikacijskih usluga podrazumijeva rizik od zlouporabe i nezakonitog pristupa.

74 Glede ciljeva koji mogu opravdati takva zadiranja, konkretno cilja zaštite nacionalne sigurnosti o kojemu je riječ u glavnom postupku, valja na početku istaknuti da je u članku 4. stavku 2. UEU-a navedeno da nacionalna sigurnost ostaje isključiva odgovornost svake države članice. Ta odgovornost odgovara primarnom interesu zaštite temeljnih državnih funkcija i temeljnih interesa društva te uključuje zaštitu i suzbijanje aktivnosti koje mogu ozbiljno destabilizirati ustavne, političke, gospodarske ili društvene strukture određene zemlje, a osobito izravno ugroziti društvo, stanovništvo ili državu kao takvu, poput, među ostalim, terorističkih aktivnosti (presuda od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 135.).

75 No, važnost cilja u vidu zaštite nacionalne sigurnosti s aspekta članka 4. stavka 2. UEU-a nadmašuje važnost drugih ciljeva iz članka 15. stavka 1. Direktive 2002/58, osobito ciljeva općenite borbe protiv kriminala, čak i teškog, kao i zaštite javne sigurnosti. Naime, opasnosti poput onih iz prethodne točke razlikuju se po svojoj naravi i posebnoj težini od općeg rizika nastanka napetosti ili poremećaja, čak i teških, glede javne sigurnosti. Pod pretpostavkom poštovanja drugih uvjeta predviđenih u članku 52. stavku 1. Povelje, cilj zaštite nacionalne sigurnosti može, stoga, opravdati mjere koje podrazumijevaju ozbiljnija zadiranja u temeljna prava od onih koja bi mogli opravdati ti drugi ciljevi (presuda od 6. listopada 2020., La Quadrature du Net i dr., C-511/18, C-512/18 i C-520/18, t. 136.).

76 Međutim, kako bi se ispunio uvjet proporcionalnosti koji je naveden u točki 67. ove presude i prema kojem odstupanja i ograničenja u zaštiti osobnih podataka moraju biti u granicama onoga što je strogo nužno, nacionalni propis kojim se zadire u temeljna prava utvrđena u člancima 7. i 8. Povelje mora poštovati zahtjeve koji proizlaze iz sudske prakse navedene u točkama 65., 67. i 68. ove presude.

77 Konkretno, glede pristupa tijela osobnim podacima, propis se ne može ograničiti na zahtjev da pristup tijela podacima odgovara cilju iz tog propisa, nego također mora predvidjeti materijalne i postupovne uvjete kojima se uređuje to korištenje (vidjeti po analogiji mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 192. i navedenu sudsku praksu).

78 Posljedično tomu, budući da se opći pristup svim zadržanim podacima, neovisno o tome postoji li ikakva veza, bilo i posredna, s ciljem koji se nastoji postići, ne može smatrati ograničenim na ono što je strogo nužno, nacionalni propis kojim je uređen pristup podacima o prometu i lokaciji mora se temeljiti na objektivnim kriterijima kako bi definirao okolnosti i uvjete u kojima nadležnim nacionalnim tijelima treba biti odobren pristup predmetnim podacima (vidjeti u tom smislu presudu od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 119. i navedenu sudsku praksu).

79 Ti se zahtjevi primjenjuju *a fortiori* na zakonsku mjeru, poput one o kojoj je riječ u glavnom postupku, a na temelju koje nacionalno nadležno tijelo može pružateljima elektroničkih komunikacijskih usluga naložiti da sigurnosnim i obavještajnim službama općenito i neselektivno prijenosom otkrivaju podatke o prometu i lokaciji. Naime, takvim se prijenosom ti podaci stavljaju na raspolaganje javnim tijelima (vidjeti po analogiji mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 212.).

80 Budući da se prijenos podataka o prometu i lokaciji obavlja općenito i neselektivno, on se sveobuhvatno tiče svih osoba koje se koriste elektroničkim komunikacijskim uslugama. On se, dakle, primjenjuje čak i na osobe za koje ne postoji nikakva naznaka koja bi navela na mišljenje da njihovo ponašanje može imati vezu, čak i posrednu ili daleku, s ciljem zaštite nacionalne sigurnosti, a osobito ako pri tome nije uspostavljen odnos između podataka čiji je prijenos predviđen i prijetnje nacionalnoj sigurnosti (vidjeti u tom smislu presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 57. i 58., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15,

EU:C:2016:970, t. 105.). S obzirom na činjenicu da je, u skladu s onim što je utvrđeno u točki 79. ove presude, prijenos takvih podataka javnim tijelima izjednačen s pristupom, valja zaključiti da propis koji omogućuje općenit i neselektivan prijenos podataka javnim tijelima podrazumijeva općenit pristup.

81 Iz toga proizlazi da nacionalni propis koji pružateljima elektroničkih komunikacijskih usluga nalaže da sigurnosnim i obavještajnim službama općenito i neselektivno prijenosom otkrivaju podatke o prometu i lokaciji, prekoračuje granice onog što je strogo nužno i ne može se smatrati opravdanim u demokratskom društvu, kao što to zahtijeva članak 15. stavak 1. Direktive 2002/58, u vezi s člankom 4. stavkom 2. UEU-a i člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje.

82 S obzirom na sva prethodna razmatranja, na drugo pitanje valja odgovoriti da članak 15. stavak 1. Direktive 2002/58, u vezi s člankom 4. stavkom 2. UEU-a, kao i člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje treba tumačiti na način da mu se protivi nacionalni propis koji državnom tijelu omogućuje da radi zaštite nacionalne sigurnosti nalaže pružateljima elektroničkih komunikacijskih usluga da sigurnosnim i obavještajnim službama općenito i neselektivno prenose podatke o prometu i lokaciji.

Troškovi

83 Budući da ovaj postupak ima značaj prethodnog pitanja za stranke glavnog postupka pred sudom koji je uputio zahtjev, na tom je sudu da odluči o troškovima postupka. Troškovi podnošenja očitovanja Sudu, koji nisu troškovi spomenutih stranaka, ne nadoknađuju se.

Slijedom navedenog, Sud (veliko vijeće) odlučuje:

1. **Članak 1. stavak 3., članak 3. i članak 15. stavak 1. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009., u vezi s člankom 4. stavkom 2. UEU-a, treba tumačiti na način da je područjem primjene te direktive obuhvaćen nacionalni propis koji državnom tijelu omogućuje da nalaže pružateljima elektroničkih komunikacijskih usluga da radi zaštite nacionalne sigurnosti prenose sigurnosnim i obavještajnim službama podatke o prometu i lokaciji.**

2. **Članak 15. stavak 1. Direktive 2002/58, kako je izmijenjena Direktivom 2009/136, u vezi s člankom 4. stavkom 2. UEU-a, kao i člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da mu se protivi nacionalni propis koji državnom tijelu omogućuje da radi zaštite nacionalne sigurnosti nalaže pružateljima elektroničkih komunikacijskih usluga da sigurnosnim i obavještajnim službama općenito i neselektivno prenose podatke o prometu i lokaciji.**

Potpisi