



## Zbornik sudske prakse

PRESUDA SUDA (veliko vijeće)

21. prosinca 2016.\*

„Zahtjev za prethodnu odluku – Elektroničke komunikacije – Obrada osobnih podataka – Povjerljivost elektroničkih komunikacija – Zaštita – Direktiva 2002/58/EZ – Članci 5., 6. i 9. i članak 15. stavak 1. – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 11. i članak 52. stavak 1. – Nacionalno zakonodavstvo – Pružatelji elektroničkih komunikacijskih usluga – Obveza koja se odnosi na opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji – Nacionalna tijela – Pristup podacima – Nepostojanje prethodnog nadzora suda ili nadzora neovisnog upravnog tijela – Usklađenost s pravom Unije“

U spojenim predmetima C-203/15 i C-698/15,

povodom zahtjeva za prethodnu odluku na temelju članka 267. UFEU-a, koje su uputili Kammarrätten i Stockholm (Upravni žalbeni sud u Stockholmu, Švedska) i Court of Appeal (England & Wales) (Civil Division) (Žalbeni sud (Engleska i Wales) (Građanski odjel), Ujedinjena Kraljevina), odlukama od 29. travnja 2015. i 9. prosinca 2015., koje je Sud zaprimio 4. svibnja 2015. i 28. prosinca 2015., u postupcima

**Tele2 Sverige AB (C-203/15)**

protiv

**Post- och telestyrelsen,**

i

**Secretary of State for the Home Department (C-698/15)**

protiv

**Toma Watsona,**

**Petera Bricea,**

**Geoffreyja Lewisa,**

uz sudjelovanje:

**Open Rights Group,**

**Privacy International,**

**The Law Society of England and Wales,**

\* \* Jezici postupka: švedski i engleski

SUD (veliko vijeće),

u sastavu: K. Lenaerts, predsjednik, A. Tizzano, potpredsjednik, R. Silva de Lapuerta, T. von Danwitz (izvjestitelj), J. L. da Cruz Vilaça, E. Juhász i M. Vilaras, predsjednici vijeća, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen i C. Lycourgos, suci,

nezavisni odvjetnik: H. Saugmandsgaard Øe,

tajnik: C. Strömholm, administratorica,

uzimajući u obzir odluku predsjednika Suda od 1. veljače 2016. da se u predmetu C-698/15 odluči u hitnom postupku iz članka 105. stavka 1. Poslovnika Suda,

uzimajući u obzir pisani postupak i nakon rasprave održane 12. travnja 2016.,

uzimajući u obzir očitovanja koja su podnijeli:

- za Tele2 Sverige AB, M. Johansson i N. Torgerzon, *advokater*, E. Lagerlöf i S. Backman,
- za T. Watsona, J. Welch i E. Norton, *solicitors*, I. Steele, *advocate*, B. Jaffey, *barrister*, i D. Rose, *QC*,
- za P. Bricea i G. Lewisa, A. Suterwalla i R. de Mello, *barristers*, R. Drabble, *QC*, i S. Luke, *solicitor*,
- za Open Rights Group i Privacy International, D. Carey, *solicitor*, R. Mehta i J. Simor, *barristers*,
- za The Law Society of England and Wales, T. Hickman, *barrister*, i N. Turner,
- za švedsku vladu, A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren i L. Swedenborg, u svojstvu agenata,
- za vladu Ujedinjene Kraljevine, S. Brandon, L. Christie i V. Kaye, u svojstvu agenata, uz asistenciju D. Bearda, G. Facenna, J. Eadieja, *QC*, i S. Ford, *barrister*,
- za belgijsku vladu, J.-C. Halleux, S. Vanrie i C. Pochet, u svojstvu agenata,
- za češku vladu, M. Smolek i J. Vláčil, u svojstvu agenata,
- za dansku vladu, C. Thorning i M. Wolff, u svojstvu agenata,
- za njemačku vladu, T. Henze, M. Hellmann i J. Kemper, u svojstvu agenata, uz asistenciju M. Kottmanna i U. Karpensteina, *Rechtsanwälte*,
- za estonsku vladu, K. Kraavi-Käerdi, u svojstvu agenta,
- za Irsku, E. Creedon, L. Williams i A. Joyce, u svojstvu agenata, uz asistenciju D. Fennellyja, *BL*,
- za španjolsku vladu, A. Rubio González, u svojstvu agenta,
- za francusku vladu, G. de Bergues, D. Colas, F.-X. Bréchet i C. David, u svojstvu agenata,
- za ciparsku vladu, K. Kleanthous, u svojstvu agenta,
- za mađarsku vladu, M. Fehér i G. Koós, u svojstvu agenata,

- za nizozemsku vladu, M. Bulterman, M. Gijzen i J. Langer, u svojstvu agenata,
- za poljsku vladu, B. Majczyna, u svojstvu agenta,
- za finsku vladu, J. Heliskoski, u svojstvu agenta,
- za Europsku komisiju, H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira i J. Vondung, u svojstvu agenata,

saslušavši mišljenje nezavisnog odvjetnika na raspravi održanoj 19. srpnja 2016.,

donosi sljedeću

### Presudu

- 1 Zahtjevi za prethodnu odluku odnose se na tumačenje 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.; u daljnjem tekstu: Direktiva 2002/58), u vezi s člancima 7. i 8. kao i člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja).
- 2 Zahtjevi su upućeni u okviru dvaju sporova, od kojih se prvi vodi između društva Tele2 Sverige AB i Post- och telestyrelsen (švedsko tijelo za nadzor pošte i telekomunikacija, u daljnjem tekstu: PTS), povodom naloga koji je potonje uputilo društvu Tele2 Sverige da provede zadržavanje podataka o lokaciji svojih pretplatnika i registriranih korisnika (predmet C-203/15), dok se drugi vodi između Toma Watsona, Petera Bricea i Geoffreyja Lewisa, s jedne strane, i Secretary of State for the Home Department (ministar unutarnjih poslova, Ujedinjena Kraljevina Velike Britanije i Sjeverne Irske), s druge strane, o usklađenosti članka 1. Data Retention and Investigatory Powers Acta 2014 (Zakon iz 2014. o zadržavanju podataka i istražnim ovlastima, u daljnjem tekstu: DRIPA) s pravom Unije (predmet C-698/15).

### Pravni okvir

#### *Pravo Unije*

Direktiva 2002/58

- 3 Uvodne izjave 2., 6., 7., 11., 21., 22., 26. i 30. Direktive 2002/58 navode:

„(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. [navedene].

[...]

- (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/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.)], ova Direktiva ne obuhvaća pitanja zaštite temeljnih prava i sloboda koje se odnose na aktivnosti koje nisu uređene pravom Zajednice. 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, 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.

[...]

- (21) Treba poduzeti mjere kako bi se spriječio neovlašten pristup komunikacijama putem javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga, s ciljem zaštite povjerljivosti komunikacija, uključujući sadržaj te podatke koji se odnose na takve komunikacije. Nacionalna zakonodavstva u pojedinim državama članicama zabranjuju samo namjeran neovlašten pristup komunikacijama.
- (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. [...]

[...]

- (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. [...]

[...]

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

4 Članak 1. Direktive 2002/58, naslovljen „Područje primjene”, propisuje:

„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 Zajednici.

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 Ugovora o osnivanju Europske zajednice, poput onih obuhvaćenih glava 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.”

5 Članak 2. Direktive 2002/58, naslovljen „Definicije”, određuje:

„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.

Također se primjenjuju sljedeće definicije:

[...]

(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;

[...]”

6 Članak 3. Direktive 2002/58, naslovljen „Dotične usluge”, određuje:

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

7 Članak 4. te direktive, naslovljen „Sigurnost obrade”, glasi:

„1. Davatelj javno dostupnih elektroničkih komunikacijskih usluga mora poduzeti odgovarajuće tehničke i organizacijske mjere kako bi zaštitio sigurnost svojih usluga, ako je potrebno zajedno s davateljem javne komunikacijske mreže, u vezi sa sigurnošću mreže. Uzimajući u obzir najnovija dostignuća i trošak njihove provedbe, ove mjere moraju osigurati razinu sigurnosti koja odgovara prikazanim opasnostima.

1a. Ne dovodeći u pitanje Direktivu [95/46], mjere navedene u stavku 1. barem:

- osiguravaju da osobnim podacima može pristupiti samo ovlašteno osoblje, za potrebe koje su zakonski odobrene,
- osiguravaju zaštitu osobnih podataka koji se pohranjuju ili prenose od nenamjernog ili protuzakonitog uništavanja, slučajnoga gubitka, mijenjanja, neovlaštenog ili nezakonitog pohranjivanja, obrade, pristupa ili razotkrivanja, i,
- osiguravaju provedbu sigurnosne politike s obzirom na obradu osobnih podataka,

[...]”

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”, propisuje:

„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 prijevара, 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”, u stavku 1. određuje:

„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 Članak 15. navedene direktive, naslovljen „Primjena određenih odredaba Direktive [95/46]”, propisuje:

„1. 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 Zajednice, uključujući ona iz članka 6. stavaka 1. i 2. Ugovora o Europskoj uniji.

[...]

1.b Operatori uspostavljaju unutarnje postupke za odgovaranje na zahtjeve za pristup osobnim podacima korisnika na temelju nacionalnih odredbi koje su usvojene u skladu sa stavkom 1. Na zahtjev državnih zakonodavnih tijela, oni također podnose podatke vezane uz navedene postupke, broj zaprimljenih zahtjeva, pozivanje na pravnu utemeljenost i njihov odgovor.

2. Odredbe poglavlja III. o pravnim lijekovima, odgovornosti i sankcijama iz Direktive [95/46] primjenjuju se u vezi s nacionalnim odredbama donesenima prema ovoj Direktivi te u vezi s pravima pojedinaca koja proistječu iz ove Direktive.

[...]”

Direktiva 95/46

- 12 Članak 22. Direktive 95/46, koji se nalazi u poglavlju III., glasi kako slijedi:

„Ne dovodeći u pitanje pravne lijekove u upravnom postupku koji se mogu propisati, među ostalim, pred nadzornim tijelom iz članka 28. ove Direktive, prije upućivanja sudskom tijelu države članice utvrđuju pravo svake osobe na pravni lijek za slučaj kršenja prava koje joj je osigurano nacionalnim pravom koje se primjenjuje na tu obradu.”

Direktiva 2006/24/EZ

- 13 Članak 1. stavak 2. Direktive 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (SL 2006., L 105, str. 54.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 50., str. 30.), naslovljen „Predmet i područje primjene”, određuje:

„Ova se Direktiva primjenjuje na podatke o prometu i lokaciji kako pravnih tako i fizičkih osoba te na uz to vezane podatke nužne za identificiranje pretplatnika ili registriranog korisnika. Ona se ne primjenjuje na sadržaj elektroničke komunikacije kao ni na informacije do kojih se dolazi korištenjem elektroničke komunikacijske mreže.”

- 14 Sukladno članku 3. te direktive, naslovljenom „Obveza zadržavanja podataka”:

„1. Iznimno od odredaba članka 5., 6. i 9. Direktive [2002/58], države članice donose mjere kojima se osigurava da se podaci iz članka 5. ove Direktive, ako su nastali pri ili su ih obradili pružatelji javno dostupnih elektroničkih komunikacijskih usluga ili javne komunikacijske mreže unutar njihove nadležnosti prilikom pružanja predmetnih komunikacijskih usluga, zadržavaju u skladu s odredbama ove Direktive.

2. Obveza zadržavanja podataka iz stavka 1. uključuje zadržavanje podataka iz članka 5. koji se odnose na neuspješne pozive kada su ti podaci nastali pri ili su ih obradili te pohranili (kada se radi o podacima o telefoniji) ili zabilježili (kada se radi o internetskim podacima) pružatelji javno dostupnih elektroničkih komunikacijskih usluga ili javne komunikacijske mreže u nadležnosti predmetne države članice prilikom pružanja predmetnih komunikacijskih usluga. Ova Direktiva ne zahtijeva da se zadržavaju podaci koji se odnose na nespojene pozive.”

*Švedsko pravo*

- 15 Iz odluke kojom se upućuje prethodno pitanje u predmetu C-203/15 proizlazi da je švedski zakonodavac, kako bi prenio Direktivu 2006/24 u nacionalno pravo, izmijenio lagen (2003:389) om elektronisk kommunikation (Zakon (2003:389) o elektroničkim komunikacijama, u daljnjem tekstu: LEK) i förordningen (2003:396) om elektronisk kommunikation (Uredba (2003:396) o elektroničkim komunikacijama). I jedan i drugi propis, u svojim verzijama koje se primjenjuju na glavni postupak, sadržavaju pravila o zadržavanju podataka o elektroničkim komunikacijama i o pristupu nacionalnih tijela tim podacima.
- 16 Pristup navedenim podacima, nadalje, uređen je u lagenu (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Zakon (2012:278) o prikupljanju podataka o elektroničkim komunikacijama u okviru istražnih djelatnosti tijela kaznenog progona, u daljnjem tekstu: Zakon 2012:278) kao i u rättegångsbalkenu (Zakon o sudskom postupku, u daljnjem tekstu: RB).



## O obvezi zadržavanja podataka o elektroničkim komunikacijama

- 17 Prema navodima suda koji je uputio zahtjev u predmetu C-203/15, odredbe članka 16.a poglavlja 6. LEK-a, u vezi s člankom 1. poglavlja 2. tog zakona, propisuju obvezu pružatelja elektroničkih komunikacijskih usluga da zadržavaju podatke čije se zadržavanje propisuje Direktivom 2006/24. Radi se o podacima o pretplatama i svim elektroničkim komunikacijama potrebnima za pronalaženje i identifikaciju izvora i odredišta komunikacije, za utvrđivanje datuma, vremena, trajanja i naravi komunikacije, za identifikaciju upotrijebljene komunikacijske opreme kao i za otkrivanje lokacije mobilne komunikacijske opreme upotrijebljene na početku komunikacije i na njezinu završetku. Obveza zadržavanja podataka odnosi se na podatke koji su dobiveni ili su obrađeni u okviru telefonske usluge, telefonske usluge putem mobilne veze, sustava elektroničkih poruka, usluge pristupa internetu kao i usluge pružanja kapaciteta za pristup internetu (način povezivanja). Ta obveza također uključuje podatke o neuspješnim komunikacijama. Ona se, međutim, ne odnosi na sadržaj komunikacija.
- 18 Članci 38. do 43. Uredbe (2003:396) o elektroničkim komunikacijama određuju kategorije podataka koji moraju biti zadržani. Kad je riječ o telefonskim uslugama, trebaju se osobito zadržavati podaci o pozivima i pozivanim brojevima kao i datumima i satima početka i završetka komunikacije koji se mogu utvrditi. Kad je riječ o telefonskim uslugama putem mobilne veze, nametnute su dodatne obveze poput, primjerice, zadržavanja podataka o lokaciji početka i završetka komunikacije. Kad je riječ o telefonskim uslugama koje sadržavaju IP paket, uz navedene, trebaju biti zadržani podaci o IP adresama pozivatelja i primatelja. Kad je riječ o sustavima elektroničkog slanja poruka, moraju se, među ostalim, zadržavati podaci o brojevima pošiljatelja i primatelja, IP adrese ili bilo koje druge adrese slanja poruka. Kad je riječ o uslugama pristupa internetu, moraju se, primjerice, zadržavati podaci o IP adresama korisnika kao i datumi i sati povezivanja na uslugu pristupa internetu koji se mogu utvrditi te datumi i sati prekida te usluge.

## O razdoblju zadržavanja podataka

- 19 U skladu s člankom 16.d poglavlja 6. LEK-a, pružatelji elektroničkih komunikacijskih usluga moraju zadržati podatke na koje se odnosi članak 16.a tog poglavlja tijekom šest mjeseci počevši od dana završetka komunikacije. Nakon toga ti se podaci trebaju odmah obrisati, osim ako je u članku 16.d drugom stavku navedenog poglavlja drukčije određeno.

## O pristupu zadržanim podacima

- 20 Pristup podacima koje su zadržala nacionalna tijela uređen je odredbama Zakona 2012:278, LEK-a i RB-a.

– Zakon 2012:278

- 21 U okviru svojih istražnih aktivnosti, nacionalna policija, Säkerhetspolisen (Sigurnosna služba, Švedska) i Tullverket (Carinska uprava, Švedska) mogu, na temelju članka 1. Zakona br. 2012:278, pod propisanim uvjetima i bez znanja pružatelja elektroničke komunikacijske mreže ili elektroničke komunikacijske usluge odobrene na temelju LEK-a, prikupljati podatke o porukama poslanima u elektroničkoj komunikacijskoj mreži, o elektroničkoj komunikacijskoj opremi na određenom zemljopisnom području kao i na zemljopisnom području ili područjima gdje se nalazi ili se nalazila ta oprema.
- 22 U skladu s člancima 2. i 3. Zakona br. 2012:278, podaci se u načelu mogu prikupljati ako su okolnosti takve da je mjera osobito potrebna kako bi se izbjegle, spriječile ili otkrile kriminalne aktivnosti koja uključuju jedno ili više kaznenih djela za koja je propisana kazna zatvora u trajanju od najmanje dvije godine ili jedna od radnji navedenih u članku 3. tog zakona, uključujući kaznena djela za koja je

propisana kazna zatvora od najmanje dvije godine. Razlozi za takvu mjeru moraju prevagnuti nad povredom prava ili štetom koja se tom mjerom može nanijeti onomu na koga se odnosi ili interesu koji joj se protivi. U skladu s člankom 5. navedenog zakona, mjera ne smije trajati više od jednog mjeseca.

23 Odluka o provođenju takve mjere jest na ravnatelju dotičnog tijela ili drugoj osobi kojoj je ta ovlast delegirana. Ona ne podliježe prethodnom nadzoru suda ili neovisnog upravnog tijela.

24 Na temelju članka 6. Zakona br. 2012:278, Säkerhets och integritetsskyddsmynden (Komisija za sigurnost i zaštitu integriteta, Švedska) mora biti obaviješten o svakoj odluci kojom se odobrava prikupljanje podataka. U skladu s člankom 1. lagena (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Zakon (2007:980) o nadzoru određenih aktivnosti kaznenog progona), to tijelo izvršava nadzor nad primjenom zakona od strane tijela kaznenog progona.

– LEK

25 Na temelju članka 22. stavka 1. točke 2. poglavlja 6. LEK-a, svaki pružatelj elektroničkih komunikacijskih usluga mora na zahtjev državnog odvjetništva, nacionalne policije, sigurnosne službe ili bilo kojeg drugog javnog tijela za kazneni progon priopćiti podatke o pretplati, ako se oni odnose na navodno počinjeno kazneno djelo. Prema navodima suda koji je uputio zahtjev u predmetu C-203/15, nije potrebno da se radi o teškom kaznenom djelu.

– RB

26 RB uređuje priopćavanje zadržanih podataka nacionalnim tijelima u okviru predistražnih radnji. U skladu s člankom 19. poglavlja 27. RB-a, „stavljanje pod nadzor elektroničkih komunikacija” bez znanja treće osobe u načelu se odobrava u okviru predistražnih radnji koje se odnose, među ostalim, na kaznena djela za koja je propisana kazna zatvora u trajanju od najmanje šest mjeseci. Pod „stavljanjem pod nadzor elektroničkih komunikacija”, u skladu s člankom 19. poglavlja 27. RB-a, valja razumjeti dobivanje podataka, bez znanja treće osobe, o poruci poslanoj elektroničkom komunikacijskom mrežom, o elektroničkoj komunikacijskoj opremi koja se nalazi ili se nalazila na određenom zemljopisnom području kao i o zemljopisnom području ili područjima gdje se nalazi ili se nalazila određena elektronička komunikacijska oprema.

27 Prema navodima suda koji je uputio zahtjev u predmetu C-203/15, informacije o sadržaju poruke ne mogu se dobiti na temelju članka 19. poglavlja 27. RB-a. U načelu, stavljanje elektroničkih komunikacija pod nadzor, na temelju članka 20. poglavlja 27. RB-a, može se odrediti samo uz postojanje opravdanih razloga za sumnju da je neka osoba počinitelj kaznenog djela i da je mjera osobito potrebna u istrazi, s obzirom na to da se potonja mora nadalje odnositi na kazneno djelo za koje je propisana kazna zatvora u trajanju od najmanje dvije godine ili na pokušaj, pripremanje ili dogovor za počinjenje takvog djela. U skladu s člankom 21. poglavlja 27. RB-a, državno odvjetništvo, osim u hitnom slučaju, mora od nadležnog suda zahtijevati odobrenje za provođenje nadzora elektroničkih komunikacija.

O sigurnosti i zaštiti zadržanih podataka

28 Na temelju članka 3.a poglavlja 6. LEK-a, pružatelji elektroničkih komunikacijskih usluga koji podliježu obvezi zadržavanja podataka moraju poduzeti tehničke i organizacijske mjere prikladne za osiguranje zaštite podataka prilikom njihove obrade. Prema navodima suda koji je uputio zahtjev u predmetu C-203/15, švedsko pravo ipak ne sadržava odredbe koje se odnose na to gdje podaci trebaju biti zadržavani.

## *Pravo Ujedinjene Kraljevine*

### DRIPA

<sup>29</sup> Članak 1. DRIPA-e, naslovljen „Ovlasti u području zadržavanja podataka o relevantnim komunikacijama, u skladu s jamstvima”, određuje:

„1. [Ministar unutarnjih poslova] može, na temelju akta („akt kojim se određuje zadržavanje”) zahtijevati od javnog telekomunikacijskog operatora da zadrži relevantne podatke o komunikacijama ako ocijeni da je to nužno i proporcionalno za ispunjavanje jednog ili više ciljeva iz točaka (a) do (h) odjeljka 22. stavka 2. Regulation of Investigatory Powers Acta 2000 (Zakon iz 2000. o istražnim ovlastima) (ciljevi zbog kojih mogu biti dobiveni podaci o komunikacijama).

2. Akt kojim se određuje zadržavanje može:

- (a) se odnositi na određenog operatora ili bilo koju kategoriju operatora;
- (b) odrediti zadržavanje svih podataka ili bilo koje kategorije podataka;
- (c) odrediti razdoblje ili razdoblja tijekom kojih podaci moraju biti zadržani;
- (d) sadržavati druge zahtjeve ili ograničenja u odnosu na zadržavanje podataka;
- (e) propisati različite odredbe u različite svrhe;
- (f) se odnositi na podatke, bez obzira na to postoje li ili ne na dan kad je akt kojim se određuje zadržavanje donesen ili stupa na snagu.

3. [Ministar unutarnjih poslova] može uredbama propisati daljnja pravila koja se odnose na zadržavanje relevantnih podataka o komunikacijama.

4. Te odredbe mogu se osobito odnositi na:

- (a) zahtjeve koji prethode donošenju akta kojim se određuje zadržavanje;
- (b) maksimalno trajanje razdoblja tijekom kojeg podaci trebaju biti zadržani na temelju akta kojim se određuje zadržavanje;
- (c) sadržaj, donošenje, stupanje na snagu, preispitivanje, izmjenu ili opoziv akta kojim se određuje zadržavanje;
- (d) integritet, sigurnost ili zaštitu zadržanih podataka na temelju ovog članka, pristup tim podacima kao i njihovo razotkrivanje ili uništenje;
- (e) provedbu relevantnih zahtjeva ili ograničenja ili provjeru usklađenosti s tim zahtjevima ili ograničenjima;
- (f) kodeks dobre prakse koji se odnosi na relevantne zahtjeve, ograničenja ili ovlasti;
- (g) povrat od strane [ministra unutarnjih poslova] (pod određenim uvjetima ili bez njih) troškova koje je snosio javni telekomunikacijski operator radi usklađivanja s relevantnim zahtjevima ili ograničenjima;

(h) činjenicu da [Data Retention (EC Directive) Regulations 2009 (Uredba iz 2009. o zadržavanju podataka na temelju direktive EZ)] prestaje važiti i da se prelazi na zadržavanje podataka na temelju ovog članka.

5. Maksimalno trajanje razdoblja određenog na temelju stavka 4. točke (b) ne smije biti duže od 12 mjeseci počevši od datuma određenog u vezi s podacima na koje se odnose uredbe iz stavka 3.

[...]”

30 Članak 2. DRIPA-e definira izraz „relevantni podaci o komunikacijama” tako da obuhvaća „relevantne podatke o komunikacijama takve vrste koja se spominje u prilogu Uredbi iz 2009. o zadržavanju podataka na temelju direktive EZ, pod uvjetom da te podatke u Ujedinjenoj Kraljevini dobivaju ili obrađuju javni telekomunikacijski operatori, u okviru pružanja predmetnih telekomunikacijskih usluga”.

RIPA

31 Članak 21. Zakona iz 2000. o istražnim ovlastima (u daljnjem tekstu: RIPA), koji se nalazi u njegovu poglavlju II. te je naslovljen „Dobivanje i razotkrivanje podataka o komunikacijama”, u stavku 4. određuje:

„U ovom poglavlju izraz ‚podaci o komunikacijama’ znači bilo što od navedenog:

- (a) bilo koji podatak o prometu sadržan u komunikaciji ili joj priložen (bilo 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 ne spada u točke (a) ili (b) koju je zadržala ili dobila u vezi s primateljima usluge osoba koja pruža poštansku ili telekomunikacijsku uslugu.”

32 Prema navodima sadržanima u odluci kojom se upućuje prethodno pitanje u predmetu C-698/15, ti podaci uključuju „podatke o lokaciji korisnika”, ali ne i one o sadržaju komunikacije.

33 Kad je riječ o pristupu zadržanim podacima, članak 22. RIPA-e određuje:

„1. Taj članak odnosi se na slučaj kad osoba odgovorna u svrhu tog poglavlja ocijeni da je zbog razloga navedenih u stavku 2. ovog članka potrebno dobiti sve podatke o komunikaciji.

2. Zbog razloga iznesenih u ovom stavku treba dobiti podatke o komunikacijama ako su potrebni:

- (a) u interesu nacionalne sigurnosti;
- (b) u svrhu sprečavanja ili otkrivanja kaznenih djela ili sprečavanja nereda;
- (c) radi gospodarskih interesa Ujedinjene Kraljevine;

- (d) u interesu javne sigurnosti;
- (e) u svrhu zaštite javnog zdravlja;
- (f) u svrhu utvrđivanja porezne osnovice ili ubiranja bilo kojeg poreza, pristojbe, naknade ili drugog nameta, doprinosa ili troška koji treba platiti javnoj upravi;
- (g) u svrhu sprečavanja – u hitnom slučaju – smrti, ozljeda ili bilo kakve štete za tjelesno ili duševno zdravlje fizičke osobe ili ublažavanja bilo kakve ozljede ili štete za tjelesno ili duševno zdravlje fizičke osobe;
- (h) u bilo koju drugu svrhu (koja ne spada u točke (a) do (g)) određenu u nalogu [ministra unutarnjih poslova].

4. Ako u stavku 5. nije drukčije uređeno, odgovorna osoba, kad joj se čini da telekomunikacijski ili poštanski operator raspolaže, može raspolagati ili bi mogao raspolagati podacima, može od njega zahtijevati da:

- (a) dobije podatke, ako već njima ne raspolaže i
- (b) razotkrije, u svakom slučaju, sve podatke kojima raspolaže ili koje je naknadno dobio.

5. Odgovorna osoba ne smije dati odobrenje u skladu sa stavkom 3. ili podnijeti zahtjev na temelju stavka 4. osim ako smatra da je dobivanje predmetnih podataka, koje se temelji na ponašanju koje je odobreno ili se zahtijeva na temelju odobrenja ili zahtjeva, proporcionalno cilju dobivanja podataka.”

<sup>34</sup> U skladu s člankom 65. RIPA-e, pritužbe se mogu podnijeti Investigatory Powers Tribunalu (Sud za istražne ovlasti, Ujedinjena Kraljevina) ako postoji razlog za zaključak da su podaci dobiveni na neprikladan način.

#### Data Retention Regulations 2014

<sup>35</sup> Data Retention Regulations 2014 (Uredba iz 2014. o zadržavanju podataka), donesen na temelju DRIPA-e, dijeli se na tri dijela, pri čemu drugi obuhvaća članke 2. do 14. te uredbe. Članak 4., naslovljen „Zahtjevi u području zadržavanja”, propisuje:

„1. U zahtjevima za zadržavanje moraju biti navedeni:

- (a) javni telekomunikacijski operator (ili opis operatora) na kojeg se odnose
- (b) podaci o relevantnim komunikacijama koji trebaju biti zadržani,
- (c) razdoblje ili razdoblja tijekom kojih podaci moraju biti zadržani,
- (d) bilo drugi zahtjev ili ograničenje u vezi sa zadržavanjem podataka.

2. U zahtjevu za zadržavanje ne može se odrediti zadržavanje podataka koje bi bilo dulje od 12 mjeseci od:

- (a) dana predmetne komunikacije u slučaju podataka o prometu ili podataka o korištenju uslugom i
- (b) dana kad je predmetna osoba okončala predmetnu komunikacijsku uslugu, u slučaju podataka o pretplatnicima, ili od dana kad je podatak izmijenjen (ako je potonji nastupio ranije).

[...]”

36 Prema članku 7. te uredbe, naslovljenom „Integritet i sigurnost podataka”:

„1. Javni telekomunikacijski operator koji zadržava podatke na temelju članka 1. [DRIPA-a] mora:

- (a) osigurati da podaci imaju isti integritet te podliježu najmanje istoj razini sigurnosti i zaštite kao i podaci sustava iz kojih dolaze,
- (b) osigurati prikladnim tehničkim i organizacijskim mjerama da samo posebno ovlašteno osoblje ima pristup podacima i
- (c) prikladnim tehničkim i organizacijskim mjerama zaštititi podatke od nezakonitog uništenja, slučajnog gubitka ili oštećivanja ili od nezakonitog ili neovlaštenog zadržavanja, obrade, pristupa ili razotkrivanja.

2. Javni telekomunikacijski operator koji zadržava podatke o komunikacijama na temelju članka 1. [DRIPA-a] mora ih uništiti ako njihovo zadržavanje više nije dopušteno tim člankom niti je na drugi način dopušteno zakonom.

3. Zahtjev iz stavka 2. za uništavanje podataka sastoji se od njihova brisanja tako da im više nije moguće pristupiti.

4. Dovoljno je da operator poduzme radnje kako bi se brisanje podataka provodilo mjesečno ili u kraćim intervalima, u skladu s njegovim mogućnostima.”

37 Članak 8. navedene uredbe, naslovljen „Razotkrivanje zadržanih podataka”, određuje:

„1. Javni telekomunikacijski operator mora uspostaviti prikladne sigurnosne sustave (koji obuhvaćaju tehničke i organizacijske mjere) kojima se određuje pristup podacima o komunikacijama zadržanima na temelju članka 1. [DRIPA-a] kako bi se spriječilo bilo kakvo razotkrivanje koje nije obuhvaćeno člankom 1. stavkom 6. točkom (a) [DRIPA-a].

2. Javni telekomunikacijski operator koji zadržava podatke na temelju članka 1. [DRIPA-a] mora ih zadržavati tako da ih na zahtjev može prenijeti bez nepotrebnog odgađanja.”

38 Članak 9. te iste uredbe, naslovljen „Nadzor povjerenika za informacije”, glasi:

„Povjerenik za informacije mora nadzirati poštovanje zahtjeva ili ograničenja propisanih u tom dijelu u vezi s integritetom, sigurnošću ili uništenjem podataka zadržanih na temelju članka 1. [DRIPA-e].”

Kodeks dobre prakse

39 Acquisition and Disclosure of Communications Data Code of Practice (Kodeks dobre prakse prilikom dobivanja i razotkrivanja podataka o komunikacijama, u daljnjem tekstu: Kodeks dobre prakse) u točkama 2.5 do 2.9 i 2.36 do 2.45 sadržava upute o potrebi i proporcionalnosti dobivanja podataka o komunikacijama. Prema pojašnjenjima suda koji je uputio zahtjev u predmetu C-698/15, osobita pozornost mora se, u skladu s točkama 3.72 do 3.77 tog kodeksa, pridati nužnosti i proporcionalnosti kad se traženi podaci o komunikacijama odnose na osobu koja je pripadnik profesije koja ima pravo na informacije zaštićene profesionalnom tajnom ili druge povjerljive informacije.

- 40 Na temelju točaka 3.78 do 3.84 navedenog kodeksa, u posebnom slučaju zahtjeva koji se odnosi na podatke o komunikacijama podnesenog kako bi se utvrdio novinarski izvor potrebno je sudsko rješenje. Prema točkama 3.85 do 3.87 istog kodeksa, u slučaju da zahtjev za pristup podnesu lokalna tijela, potrebno je sudsko odobrenje. S druge strane, nikakvo sudsko odobrenje ili odobrenje neovisnog tijela nije potrebno kad je riječ o pristupu podacima o komunikacijama zaštićenima profesionalnom tajnom na temelju zakona ili onima koji se odnose na liječnike, članove Parlamenta ili svećenike.
- 41 Točka 7.1 kodeksa dobre prakse predviđa da podaci o komunikacijama koji su stečeni ili dobiveni na temelju odredbi RIPA-e kao i svi izvaci, sažeci i preslike tih podataka moraju biti obrađeni i pohranjeni na siguran način. Nadalje, moraju se poštovati zahtjevi koji se nalaze u Data Protection Actu (Zakon o zaštiti podataka).
- 42 U skladu s točkom 7.18 Kodeksa dobre prakse, kad javno tijelo Ujedinjene Kraljevine razmatra moguće razotkrivanje podataka o komunikacijama stranim tijelima, ono mora, među ostalim, provjeriti hoće li se ti podaci zaštititi na prikladan način. Ipak, iz točke 7.22 tog kodeksa proizlazi da do prijenosa podataka u treće zemlje može doći kad je on potreban zbog razloga povezanih s važnim javnim interesom, čak i kad treća zemlja ne osigura prikladnu razinu zaštite. Prema navodima suda koji je uputio zahtjev u predmetu C-698/15, ministar unutarnjih poslova izdati potvrdu o nacionalnoj sigurnosti kojom se određeni podaci izuzimaju od obveze poštovanja odredbi predviđenih zakonodavstvom.
- 43 U točki 8.1. navedenog kodeksa navodi se da je RIPA-om uveden Interception of Communications Commissioner (povjerenik za presretanje komunikacija, Ujedinjena Kraljevina), čija je uloga, među ostalim, provoditi neovisan nadzor nad izvršavanjem i provedbom ovlasti i dužnosti iz poglavlja II. dijela I. RIPA-e. Kao što to proizlazi iz točke 8.3 istog kodeksa, taj povjerenik, u slučaju da može „utvrditi da je pojedinac oštećen namjernom povredom ili povredom iz nepažnje”, ovlašten je obavijestiti tog pojedinca da postoji sumnja u nezakonito izvršavanje ovlasti.

## Glavni postupci i prethodna pitanja

### *Predmet C-203/15*

- 44 Dana 9. travnja 2014. Tele2 Sverige, pružatelj elektroničkih komunikacijskih usluga sa sjedištem u Švedskoj, obavijestio je PTS da će, nakon proglašenja ništavosti Direktive 2006/24 presudom od 8. travnja 2014., Digital Rights Ireland i dr. (C-293/12 i C-594/12, u daljnjem tekstu: presuda Digital Rights, EU:C:2014:238), to društvo počevši od 14. travnja 2014. prestati zadržavati podatke koji se odnose na elektroničke komunikacije određene LEK-om i da će ukloniti podatke zadržane do tog datuma.
- 45 Dana 15. travnja 2014. Rikspolisstyrelsen (Opća uprava nacionalne policije, Švedska) podnio je PTS-u pritužbu zbog toga što mu je Tele2 Sverige prestao priopćavati predmetne podatke.
- 46 Dana 29. travnja 2014. justitieminister (ministar pravosuđa, Švedska) imenovao je posebnog izvjestitelja odgovornog za analizu predmetnog švedskog propisa u pogledu presude Digital Rights. U izvještaju od 13. lipnja 2014., naslovljenom „Datalagring, EU-rätt och svensk rätt, n° Ds 2014:23” (Zadržavanje podataka, pravo Unije i švedsko pravo, u daljnjem tekstu: Izvještaj iz 2014.), posebni izvjestitelj zaključio je da se nacionalni propis o zadržavanju podataka poput onog u člancima 16.a do 16.f LEK-a ne protivi ni pravu Unije ni Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda, potpisanoj u Rimu 4. studenoga 1950. (u daljnjem tekstu: EKLJP). Posebni izvjestitelj istaknuo je da presudu Digital Rights nije moguće tumačiti na način da je njome ograničeno samo načelo općeg i neselektivnog zadržavanja podataka. Prema tom izvjestitelju, presuda Digital Rights nije se smjela tumačiti ni na način da je Sud u njoj utvrdio niz kriterija koji bi redom morali biti zadovoljeni kako bi

se neki propis mogao smatrati proporcionalnim. Valja ocijeniti sve okolnosti kako bi se utvrdila sukladnost švedskog propisa s pravom Unije, poput opsega zadržavanja podataka s obzirom na odredbe o pristupu podacima, trajanju njihova zadržavanja te zaštiti i sigurnosti tih podataka.

- 47 Na toj osnovi, PTS je 19. lipnja 2014. obavijestio Tele2 Sverige da je povrijedio obveze iz nacionalnog propisa time što nije zadržao podatke određene u LEK-u tijekom šest mjeseci s ciljem borbe protiv kriminaliteta. Nalogom od 27. lipnja 2014. PTS mu je potom odredio da najkasnije 25. srpnja 2014. izvrši zadržavanje tih podataka.
- 48 Smatrajući da se Izvještaj iz 2014. temelji na pogrešnom tumačenju presude Digital Rights i da se obveza zadržavanja podataka protivi temeljnim pravima zajamčenima Poveljom, Tele2 Sverige podnio je tužbu Förvaltningsrättenu i Stockholm (Upravni sud u Stockholmu, Švedska) protiv naloga od 27. lipnja 2014. Budući da je taj sud odbio tužbu presudom od 13. listopada 2014., Tele2 Sverige sudu koji je uputio zahtjev podnio je žalbu na tu presudu.
- 49 Prema sudu koji je uputio zahtjev, sukladnost švedskog propisa s pravom Unije mora se ocjenjivati s obzirom na članak 15. stavak 1. Direktive 2002/58. Naime, iako ta direktiva uspostavlja načelo prema kojem podaci o prometu i lokaciji moraju biti brisani ili učinjeni anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije, članak 15. stavak 1. navedene direktive uvodi iznimku od tog načela jer ovlašćuje države članice, kad je to opravdano jednim od razloga koje navodi, da ograniče tu obvezu brisanja ili anonimiziranja ili čak odrede zadržavanje podataka. Dakle, pravo Unije u određenim okolnostima dopušta zadržavanje podataka o elektroničkim komunikacijama.
- 50 Ipak, sud koji je uputio zahtjev dvoji o tome je li opća i neselektivna obveza zadržavanja podataka o elektroničkim komunikacijama, poput one iz glavnog postupka, s obzirom na presudu Digital Rights, u skladu s člankom 15. stavkom 1. Direktive 2002/58, tumačenim u vezi s člancima 7. i 8. i člankom 52. stavkom 1. Povelje. S obzirom na različita mišljenja stranaka u tom pogledu, Sud se treba jednoznačno izjasniti o pitanju je li, kao što to smatra Tele2 Sverige, opće i neselektivno zadržavanje podataka o elektroničkim komunikacijama kao takvo protivno člancima 7. i 8. i članku 52. stavku 1. Povelje ili, kao što to proizlazi iz Izvještaja iz 2014., sukladnost takvog zadržavanja podataka treba ocjenjivati s obzirom na odredbe o pristupu podacima, njihovoj zaštiti i sigurnosti kao i trajanju njihova zadržavanja.
- 51 U tim je okolnostima sud koji je uputio zahtjev odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:
- „1. Je li opća obveza zadržavanja podataka o prometu koja obuhvaća sve osobe, sva sredstva elektroničke komunikacije i sve podatke o prometu bez ikakvih razlika, ograničenja ili iznimki u svrhu borbe protiv kriminaliteta [...] u skladu s člankom 15. stavkom 1. Direktive 2002/58, uzimajući u obzir članke 7. i 8. i članak 52. stavak 1. Povelje?
  2. U slučaju negativnog odgovora na prvo pitanje, može li se obveza zadržavanja iznimno dopustiti:
    - (a) ako je pristup nacionalnih tijela zadržanim podacima određen na način opisan u točkama 19. do 36. [odluke kojom se upućuje prethodno pitanje], i
    - (b) ako su sigurnost i zaštita podataka uređeni na način opisan u točkama 38. do 43. [odluke kojom se upućuje prethodno pitanje], i
    - (c) ako svi relevantni podaci moraju biti zadržani tijekom šest mjeseci, računajući od dana kad je komunikacija završena, te potom izbrisani, kako je opisano u točki 37. [odluke kojom se upućuje prethodno pitanje]?”



*Predmet C-698/15*

- 52 T. Watson, P. Brice i G. Lewis podnijeli su, svaki posebno, High Courtu of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Visoki sud (Engleska i Wales), odjel Queens' Bench (izdvojeno vijeće), Ujedinjena Kraljevina) zahtjev za nadzor zakonitosti članka 1. DRIPA-e, pozivajući se osobito na nesukladnost tog članka s člancima 7. i 8. Povelje kao i s člankom 8. EKLJP-a.
- 53 Presudom od 17. srpnja 2015. High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Visoki sud (Engleska i Wales), odjel Queens' Bench (izdvojeno vijeće), Ujedinjena Kraljevina) utvrdio je da su presudom Digital Rights uspostavljeni „važni zahtjevi u pravu Unije” koji su primjenjivi na propise država članica u području zadržavanja podataka o komunikacijama i pristupu takvim podacima. Prema mišljenju tog suda, budući da je Sud u toj presudi utvrdio da Direktiva 2006/24 nije u skladu s načelom proporcionalnosti, nacionalni propis čiji je sadržaj istovjetan njezinu sadržaju također ne može biti u skladu s tim načelom. Iz temeljne logike presude Digital Rights proizlazi da zakonodavstvo kojim se uspostavlja opći sustav pravila o zadržavanju podataka o komunikacijama krši prava zajamčena člancima 7. i 8. Povelje, pod uvjetom da ono nije dopunjeno sustavom pravila o pristupu podacima, definiranim nacionalnim pravom, koji predviđa dostatna jamstva za zaštitu tih prava. Članak 1. DRIPA-e nije sukladan člancima 7. i 8. Povelje, s obzirom na to da se njime ne određuju jasna i precizna pravila o pristupu zadržanim podacima i njihovu korištenju te se pristup tim podacima ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela.
- 54 Ministar unutarnjih poslova podnio je žalbu na tu presudu Courtu of Appeal (England & Wales) (Civil Division) (Žalbeni sud (Engleska i Wales) (Građanski odjel), Ujedinjena Kraljevina)).
- 55 Taj sud navodi da članak 1. stavak 1. DRIPA-e ovlašćuje ministra unutarnjih poslova da bez ikakva prethodnog sudskog odobrenja ili odobrenja neovisnog upravnog tijela donese opća pravila kojima se javnim telekomunikacijskim operatorima nalaže zadržavanje svih podataka o bilo kojoj poštanskoj ili telekomunikacijskoj usluzi u trajanju od najviše dvanaest mjeseci ako ocijeni da je takav zahtjev potreban i proporcionalan radi provedbe ciljeva utvrđenih u propisu Ujedinjene Kraljevine. Iako ti podaci ne obuhvaćaju sadržaj komunikacije, oni bi mogli osobito narušavati privatnost korisnika komunikacijskih usluga.
- 56 U odluci kojom se upućuje prethodno pitanje i u svojoj presudi od 20. studenoga 2015., donesenoj u okviru žalbenog postupka, kojom je odlučio uputiti Sudu ovaj zahtjev za prethodnu odluku, sud koji ga je uputio smatra da su nacionalna pravila o zadržavanju podataka nužno obuhvaćena člankom 15. stavkom 1. Direktive 2002/58 i stoga trebaju poštovati zahtjeve koji proizlaze iz Povelje. Međutim, u skladu s člankom 1. stavkom 3. te direktive, zakonodavac Unije nije uskladio pravila o pristupu zadržanim podacima.
- 57 Kad je riječ o učinku presude Digital Rights na pitanja iz glavnog postupka, sud koji je uputio zahtjev navodi da je u predmetu koji je doveo do te presude Sud odlučivao o valjanosti Direktive 2006/24, a ne nacionalnog propisa. Kad je riječ osobito o uskoj vezi između zadržavanja podataka i pristupa tim podacima, bilo je nužno da ta direktiva sadržava niz jamstava i da se u presudi Digital Rights prilikom ispitivanja zakonitosti pravila zadržavanja podataka utvrđenih tom direktivom analiziraju pravila o pristupu tim podacima. Sud stoga nije namjeravao u toj presudi odrediti važne zahtjeve koji se primjenjuju na nacionalne propise o pristupu podacima kojima se ne provodi pravo Unije. Nadalje, argumentacija Suda bila je usko povezana s ciljem te direktive. Nacionalni propis treba, međutim, ocjenjivati s obzirom na njegove ciljeve i kontekst.
- 58 Kad je riječ o potrebi upućivanja Sudu zahtjeva za prethodnu odluku, sud koji ga je uputio ističe činjenicu da je na dan donošenja odluke o upućivanju šest sudova drugih država članica, od kojih pet najviše instance, poništilo nacionalno zakonodavstvo na temelju presude Digital Rights. Odgovor na postavljena pitanja stoga nije očit, iako je potreban za odluku o predmetima o kojima se vodi postupak pred tim sudom.

59 U tim je uvjetima Court of Appeal (England & Wales) (Civil Division) (Žalbeni sud (Engleska i Wales) (Građanski odjel)) odlučio prekinuti postupak i postaviti Sudu sljedeća prethodna pitanja:

- „1. Uspostavlja li presuda Digital Rights (uključujući osobito točke 60. do 62.) važne zahtjeve prava Unije primjenjive na nacionalni sustav države članice koji uređuje pristup podacima zadržanima u skladu s nacionalnim zakonodavstvom s ciljem usklađivanja s člancima 7. i 8. Povelje?
2. Proširuje li presuda Digital Rights doseg članka 7. i/ili 8. Povelje u odnosu na doseg članka 8. EKLP-a kako je utvrđen sudskom praksom Europskog suda za ljudska prava?”

### **Postupak pred Sudom**

60 Rješenjem od 1. veljače 2016., Davis i dr. (C-698/15, neobjavljeno, EU:C:2016:70) predsjednik Suda odlučio je prihvatiti zahtjev koji je uputio Court of Appeal (England & Wales) (Civil Division) (Žalbeni sud (Engleska i Wales) (Građanski odjel)) da se o predmetu C-698/15 odlučuje u ubrzanom postupku iz članka 105. stavka 1. Poslovnika Suda.

61 Odlukom predsjednika Suda od 10. ožujka 2016. predmeti C-203/15 i C-698/15 spojeni su u svrhu usmenog dijela postupka i donošenja presude.

### **O prethodnim pitanjima**

#### *Prvo pitanje u predmetu C-203/15*

62 Svojim prvim pitanjem u predmetu C-203/15 Kammarrätten i Stockholm (Upravni žalbeni sud u Stockholmu) u biti pita treba li članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7. i 8. i člankom 52. stavkom 1. Povelje, tumačiti na način da mu se protivi nacionalni propis poput onoga u glavnom postupku, kojim se u svrhu borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u vezi sa svim sredstvima elektroničke komunikacije.

63 To pitanje osobito proizlazi iz činjenice da je Direktiva 2006/24, čije je prenošenje bilo cilj nacionalnog propisa iz glavnog postupka, na temelju presude Digital Rights proglašena nevaljanom, ali da stranke imaju različito mišljenje o dosegu te presude i njezinu učinku na navedeni propis, koji uređuje zadržavanje podataka o prometu i lokaciji kao i pristup nacionalnih tijela tim podacima.

64 Najprije valja ispitati spada li nacionalni propis poput onoga iz glavnog postupka u područje primjene prava Unije.

#### *Područje primjene Direktive 2002/58*

65 Države članice koje su podnijele pisana očitovanja Sudu izrazile su različita mišljenja o tome spadaju li i u kojoj mjeri nacionalni propisi o zadržavanju podataka o prometu i lokaciji i pristupu nacionalnih tijela tim podacima u svrhu borbe protiv kriminaliteta u područje primjene Direktive 2002/58. Dok su, među ostalim, belgijska, danska, njemačka, estonska, irska i nizozemska vlada izrazile mišljenje da na takvo pitanje valja odgovoriti potvrdno, češka vlada predložila je niječan odgovor, primijetivši da je jedini cilj tih propisa borba protiv kriminaliteta. Kad je riječ o vladi Ujedinjene Kraljevine, ona je navela da u područje primjene te direktive spadaju samo propisi o zadržavanju podataka, a ne oni o pristupu tim podacima nadležnih nacionalnih tijela u području kaznenog progona.

- 66 Kad je riječ, naposljetku, o Komisiji, iako je ona u pisanim očitovanjima podnesenima Sudu u predmetu C-203/15 smatrala da nacionalni propis iz glavnog postupka spada u područje primjene Direktive 2002/58, u svojim pisanim očitovanjima u predmetu C-698/15 ustvrdila je da samo nacionalna pravila o zadržavanju podataka, a ne ona o pristupu nacionalnih tijela tim podacima, spadaju u područje primjene te direktive. Komisija ipak smatra da potonja trebaju biti uzeta u obzir kako bi se ocijenilo čini li nacionalni propis kojim se uređuje zadržavanje podataka od strane pružatelja elektroničkih komunikacijskih usluga proporcionalno miješanje u temeljna prava zajamčena člancima 7. i 8. Povelje.
- 67 U tom pogledu valja navesti da se područje primjene Direktive 2002/58 mora ocjenjivati vodeći računa osobito o njezinoj općoj strukturi.
- 68 Na temelju svojeg članka 1. stavka 1., Direktiva 2002/58 predviđa, među ostalim, usklađivanje nacionalnih odredbi država članica koje trebaju osigurati ujednačenu razinu zaštite temeljnih prava i sloboda, a posebno prava na privatnost i povjerljivost u vezi s obradom osobnih podataka u području elektroničkih komunikacija.
- 69 Članak 1. stavak 3. te direktive isključuje iz njezina područja primjene „aktivnosti države” u ondje predviđenim područjima, odnosno osobito aktivnosti države u kaznenom području i područjima koja se odnose na javnu sigurnost, obranu, državnu sigurnost, uključujući gospodarsku dobrobit države kada se aktivnosti odnose na pitanja državne sigurnosti (vidjeti, analogijom, kad je riječ o članku 3. stavku 2. prvom podstavku Direktive 95/46, presude od 6. studenoga 2003., Lindqvist, C-101/01, EU:C:2003:596, t. 43. i od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, t. 41.).
- 70 Kad je riječ o članku 3. Direktive 2002/58, u njemu je određeno 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). Stoga valja smatrati da navedena direktiva uređuje aktivnosti pružatelja takvih usluga.
- 71 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”. Drugom rečenicom članka 15. stavka 1. navedene direktive primjera radi navedene su mjere koje države članice tako mogu donijeti, a „kojima se omogućuje zadržavanje podataka”.
- 72 Doista, zakonske mjere iz članka 15. stavka 1. Direktive 2002/58 odnose se na državne aktivnosti ili aktivnosti državnih tijela, koje nisu svojstvene aktivnostima pojedinaca (vidjeti u tom smislu presudu od 29. siječnja 2008., Promusicae, C-275/06, EU:C:2008:54, t. 51.). Nadalje, ciljevi kojima na temelju te odredbe takve mjere moraju težiti – u predmetnom slučaju zaštita nacionalne sigurnosti, obrane i javne sigurnosti kao i sprečavanje, istraga, otkrivanje i progon kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava – u biti se preklapaju s ciljevima aktivnosti iz članka 1. stavka 3. te direktive.
- 73 Ipak, s obzirom na opću strukturu Direktive 2002/58, elementi navedeni u prethodnoj točki ove presude ne omogućuju zaključak da su zakonske mjere iz njezina članka 15. stavka 1. isključene iz područja primjene te direktive jer bi u suprotnom navedena odredba ostala bez ikakva korisnog učinka. Ta odredba nužno pretpostavlja da nacionalne mjere koje su njome predviđene, poput onih koje se odnose na zadržavanje podataka u svrhu borbe protiv kriminaliteta, spadaju u područje primjene spomenute direktive jer potonja izričito ovlašćuje države članice da ih donesu samo uz poštovanje uvjeta koje predviđa.

- 74 Nadalje, zakonske mjere predviđene u članku 15. stavku 1. Direktive 2002/58 uređuju, u svrhu spomenutu u toj odredbi, aktivnosti pružatelja elektroničkih komunikacijskih usluga. Slijedom toga, navedenu odredbu te direktive, u vezi s njezinim člankom 3., valja tumačiti na način da takve zakonske mjere spadaju u područje njezine primjene.
- 75 U to područje primjene osobito spada zakonska mjera poput one u glavnom postupku, koja tim pružateljima nalaže zadržavanje podataka o prometu i lokaciji jer se takva aktivnost nužno odnosi na to da oni obrađuju osobne podatke.
- 76 U navedeno područje primjene spada i zakonska mjera poput one u glavnom postupku o pristupu nacionalnih tijela podacima koje su zadržali pružatelji elektroničkih komunikacijskih usluga.
- 77 Naime, zaštita povjerljivosti elektroničkih komunikacija i s njima povezanih podataka o prometu, zajamčena člankom 5. stavkom 1. Direktive 2002/58, primjenjuje se na mjere koje poduzimaju sve osobe osim korisnika, bez obzira na to radi li se o privatnim osobama odnosno tijelima ili o državnim tijelima. Kao što to potvrđuje uvodna izjava 21. te direktive, njezin je cilj spriječiti neovlašten „pristup” komunikacijama, uključujući „podatke koji se odnose na takve komunikacije”, kako bi se zaštitila povjerljivost elektroničkih komunikacija.
- 78 U tim okolnostima, zakonska mjera kojom država članica na temelju članka 15. stavka 1. Direktive 2002/58 nalaže pružateljima elektroničkih komunikacijskih usluga da, u svrhu navedenu u toj odredbi i pod uvjetima određenima u takvoj mjeri, odobri nacionalnim tijelima pristup podacima koje su zadržali navedeni pružatelji odnosi se na njihovu obradu osobnih podataka koja spada u područje primjene iste direktive.
- 79 Nadalje, budući da se zadržavanje podataka izvršava samo u svrhu da oni, prema potrebi, budu dostupni nadležnim nacionalnim tijelima, nacionalni propis kojim se određuje zadržavanje podataka u načelu nužno podrazumijeva odredbe o pristupu nadležnih nacionalnih tijela podacima koje su zadržali pružatelji elektroničkih komunikacijskih usluga.
- 80 To tumačenje potkrijepljeno je člankom 15. stavkom 1.b Direktive 2002/58, prema kojem pružatelji uspostavljaju unutarnje postupke za odgovaranje na zahtjeve za pristup osobnim podacima korisnika na temelju nacionalnih odredbi donesenih u skladu s člankom 15. stavkom 1. te direktive.
- 81 Iz prethodno navedenog proizlazi da nacionalni propis poput onoga u glavnim postupcima u predmetima C-203/15 i C-698/15 spada u područje primjene Direktive 2002/58.

Tumačenje članka 15. stavka 1. Direktive 2002/58 s obzirom na članke 7., 8. i 11. i članak 52. stavak 1. Povelje

- 82 Valja navesti da, u skladu s člankom 1. stavkom 2. Direktive 2002/58, njezine odredbe „pojašnjavaju i nadopunjuju” Direktivu 95/46. Kao što je to navedeno u njezinoj uvodnoj izjavi 2., cilj je Direktive 2002/58, među ostalim, poštovanje prava određenih 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”.
- 83 U tu svrhu, Direktiva 2002/58 sadržava posebne odredbe kojima je cilj, kao što to proizlazi, među ostalim, iz njezinih uvodnih izjava 6. i 7., zaštititi korisnike elektroničkih komunikacijskih usluga od opasnosti za osobne podatke i privatni život koje su rezultat novih tehnologija i veće sposobnosti automatskog pohranjivanja i obrade podataka.

- 84 Članak 5. stavak 1. te direktive, među ostalim, predviđa da 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.
- 85 Načelo povjerljivosti komunikacija uspostavljeno Direktivom 2002/58 podrazumijeva, među ostalim, kao što to proizlazi iz druge rečenice članka 5. stavka 1. te direktive, načelnu zabranu svim osobama koje nisu korisnici da bez pristanka potonjih pohranjuju podatke o prometu povezane s elektroničkim komunikacijama. Jedine iznimke čine osobe koje imaju zakonsko dopuštenje u skladu s člankom 15. stavkom 1. te direktive i tehničko pohranjivanje koje je nužno za prijenos komunikacije (vidjeti u tom smislu presudu od 29. siječnja 2008., *Promusicae*, C-275/06, EU:C:2008:54, t. 47.).
- 86 Stoga, kao što to potvrđuju uvodne izjave 22. i 26. Direktive 2002/58, na temelju njezina članka 6., obrada i pohrana podataka o prometu dopuštena je samo u svrhu naplaćivanja usluge, marketinga elektroničkih komunikacijskih usluga ili pružanja usluge s posebnom tarifom (vidjeti u tom smislu presudu od 29. siječnja 2008., *Promusicae*, C-275/06, EU:C:2008:54, t. 47. i 48.). Kad je osobito riječ o naplaćivanju usluga, takva je obrada dopuštena samo do kraja razdoblja tijekom kojeg se račun može pravno pobijati ili tijekom kojeg se može zahtijevati plaćanje. Nakon proteka tog razdoblja, obrađeni i pohranjeni podaci moraju se obrisati ili učiniti anonimnima. Kad je riječ o podacima o lokaciji koji nisu podaci o prometu, članak 9. stavak 1. te direktive predviđa da se oni mogu obrađivati samo pod određenim uvjetima i nakon što su učinjeni anonimnima odnosno uz pristanak korisnika ili pretplatnika.
- 87 Doseg odredbi članka 5. i 6. i članka 9. stavka 1. Direktive 2002/58, čiji je cilj zajamčiti povjerljivost komunikacija i s njima povezanih podataka te na najmanju moguću mjeru smanjiti rizik od zlorabe, treba, nadalje, ocjenjivati u vezi s uvodnom izjavom 30. te direktive, na temelju koje „sustave pružanja elektroničkih komunikacijskih mreža i usluga treba koncipirati tako da ograniče količinu nužnih osobnih podataka na strogi minimum”.
- 88 Doista, članak 15. stavak 1. Direktive 2002/58 omogućava državama članicama da uvedu iznimke od načela, propisanog u članku 5. stavku 1. te direktive, prema kojem su obvezne jamčiti povjerljivost osobnih podataka kao i iznimke od odgovarajućih obveza, spomenutih osobito u člancima 6. i 9. navedene direktive (vidjeti u tom smislu presudu od 29. siječnja 2008., *Promusicae*, C-275/06, EU:C:2008:54, t. 50.).
- 89 Ipak, u mjeri u kojoj članak 15. stavak 1. Direktive 2002/58 omogućuje državama članicama da ograniče doseg načela prema kojem su obvezne osigurati povjerljivost komunikacija i s njima povezanih podataka o prometu, treba ga, sukladno ustaljenoj sudskoj praksi Suda, usko tumačiti (vidjeti analogijom presudu od 22. studenoga 2012., *Probst*, C-119/12, EU:C:2012:748, t. 23.). Taj članak stoga ne može opravdati to da odstupanje od obveznosti tog načela i osobito od zabrane pohrane tih podataka, predviđene u članku 5. Direktive 2002/58, postane pravilo, kako potonja odredba ne bi izgubila na svojem dosegu.
- 90 U tom pogledu valja navesti da prva rečenica članka 15. stavka 1. Direktive 2002/58 predviđa da njome određene zakonske mjere kojima se odstupa od načela povjerljivosti komunikacija i s njima povezanih podataka o prometu mora za cilj imati „zaštit[u] nacionalne sigurnosti (odnosno državne sigurnosti), obrane, javne sigurnosti te sprečavanj[e], istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava” ili drugi cilj predviđen člankom 13. stavkom 1. Direktive 95/46 na koji upućuje prva rečenica članka 15. stavka 1. Direktive 2002/58 (vidjeti u tom smislu presudu od 29. siječnja 2008., *Promusicae*, C-275/06, EU:C:2008:54, t. 53.). Takvo je nabranje ciljeva iscrpno, kao što to proizlazi iz druge rečenice članka 15. stavka 1. te direktive, na temelju kojeg zakonske mjere moraju biti opravdane „razlozima određenim” u prvoj rečenici članka spomenute odredbe Direktive. Posljedično tomu, države članice ne mogu donijeti takve mjere u druge svrhe osim onih nabrojanih u potonjoj odredbi.

- 91 Nadalje, treća rečenica članka 15. stavka 1. Direktive 2002/58 određuje da „[s]ve mjere [iz navedene odredbe] moraju biti u skladu s općim načelima prava [Unije], uključujući ona iz članka 6. stavaka 1. i 2. [UEU-a]”, među kojima se nalaze opća načela i temeljna prava koja su od tada zajamčena Poveljom. Članak 15. stavak 1. Direktive 2002/58 treba, dakle, tumačiti s obzirom na temeljna prava zajamčena Poveljom (vidjeti analogijom, kad je riječ o Direktivi 95/46, presude od 20. svibnja 2003., Österreichischer Rundfunk i dr., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, t. 68.; od 13. svibnja 2014., Google Spain i Google, C-131/12, EU:C:2014:317, t. 68. i od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 38.).
- 92 U tom pogledu valja naglasiti da obveza zadržavanja podataka o prometu, koju na temelju nacionalnog propisa poput onoga u glavnom postupku imaju pružatelji elektroničkih komunikacijskih usluga, 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 su izričito spomenuti u prethodnim pitanjima, već i u vezi sa slobodom izražavanja, zajamčenom u članku 11. Povelje (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 25. i 70.).
- 93 Stoga važnost kako prava na poštovanje privatnosti zajamčenog člankom 7. Povelje tako i prava na poštovanje osobnih podataka zajamčenog njezinim člankom 8., kao što to proizlazi iz sudske prakse Suda (vidjeti u tom smislu presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 39. i navedenu sudsku praksu), mora biti uzeta u obzir prilikom tumačenja članka 15. stavka 1. Direktive 2002/58. Isto vrijedi za pravo na slobodu izražavanja, s obzirom na osobitu važnost koju ona uživa u svakom demokratskom društvu. To temeljno pravo, zajamčeno u članku 11. Povelje, jedan je 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 12. lipnja 2003., Schmidberger, C-112/00, EU:C:2003:333, t. 79. i od 6. rujna 2011., Patriciello, C-163/10, EU:C:2011:543, t. 31.).
- 94 U tom pogledu valja podsjetiti da, u skladu s člankom 52. stavkom 1. Povelje, svako ograničenje pri ostvarivanju njome priznatih prava i sloboda mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja pri ostvarivanju tih prava i sloboda moguća su samo ako su potrebna i ako stvarno odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba (presuda od 15. veljače 2016., N., C-601/15 PPU, EU:C:2016:84, t. 50.).
- 95 S obzirom na posljednjenavedeno, prva rečenica članka 15. stavka 1. Direktive 2002/58 određuje da države članice mogu donijeti mjeru kojom se odstupa od načela povjerljivosti komunikacija i s njima povezanih podataka o prometu kad ona predstavlja „nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva” s obzirom na ciljeve utvrđene tom odredbom. Kad je riječ o uvodnoj izjavi 11. te direktive, u njoj je pojašnjeno da mjera te naravi mora biti „strogo” razmjerna svrsi za koju se poduzima. U pogledu, osobito, zadržavanja podataka, druga rečenica članka 15. stavka 1. navedene direktive zahtijeva da se ono provodi „tijekom ograničenog razdoblja” i dok je „opravdano” jednim od razloga određenim u prvoj rečenici članka 15. stavka 1. te direktive.
- 96 Poštovanje načela proporcionalnosti također proizlazi iz ustaljene sudske prakse Suda prema kojoj zaštita temeljnog prava na poštovanje privatnog života na razini Unije zahtijeva da su odstupanja i ograničenja u zaštiti osobnih podataka u granicama onoga što je strogo nužno (presude od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, t. 56.; od 9. studenoga 2010., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, t. 77.; Digital Rights, t. 52. i od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 92.).
- 97 Kad je riječ o pitanju ispunjava li nacionalni propis poput onoga u predmetu C-203/15 te uvjete, valja navesti da je njime određeno opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije te da su njime pružatelji elektroničkih komunikacijskih usluga obvezni sustavno i stalno zadržavati te podatke,

i to bez bilo kakve iznimke. Kako to proizlazi iz odluke kojom se upućuje prethodno pitanje, kategorije podataka predviđene tim propisom u biti odgovaraju onima čije je zadržavanje uređeno Direktivom 2006/24.

- 98 Podaci koje trebaju zadržati pružatelji elektroničkih komunikacijskih usluga omogućavaju pronalaženje i identifikaciju izvora komunikacije i njezina odredišta, utvrđivanje datuma, vremena, trajanja i vrste komunikacije, pronalaženje i identifikaciju komunikacijske opreme korisnikâ kao i otkrivanje lokacije mobilne komunikacijske opreme. Među tim podacima nalaze se, među ostalim, ime i adresa pretplatnika ili registriranog korisnika, broj telefona pozivatelja i pozvani broj kao i IP adresa za internetske usluge. Ti podaci osobito omogućavaju saznanje s kojom je osobom pretplatnik ili registrirani korisnik komunicirao i kojim sredstvom kao i utvrđivanje vremena komunikacije i mjesta s kojeg se ona odvijala. Nadalje, oni omogućavaju uvid u učestalost komunikacija pretplatnika ili registriranog korisnika s određenim osobama tijekom danog razdoblja (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 26.).
- 99 Ti podaci, uzeti zajedno, mogu omogućiti donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podaci zadržani, kao što su svakodnevne navike, mjesta trajnih ili privremenih boravišta, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posjećivale (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 27.). Ti podaci osobito omogućuju, kao što je to naveo nezavisni odvjetnik u točkama 253., 254. i 257. do 259. svojeg mišljenja, utvrđivanje profila predmetnih osoba, što je jednako osjetljiva informacija s obzirom na pravo na poštovanje privatnog života, kao i sam sadržaj komunikacija.
- 100 Miješanje takvog propisa u temeljna prava utvrđena člancima 7. i 8. Povelje širokog je dosega i treba ga smatrati osobito ozbiljnim. Okolnost da se zadržavanje podataka izvršava a da o tome korisnici elektroničkih komunikacija nisu obaviješteni može kod dotičnih osoba stvoriti osjećaj da je njihov privatni život predmet trajnog nadzora (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 37.).
- 101 Iako takvim propisom nije odobreno zadržavanje sadržaja komunikacije te stoga ne može povrijediti bitan sadržaj navedenih prava (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 39.), zadržavanje podataka o prometu i lokaciji može ipak imati utjecaj na uporabu elektroničkih komunikacijskih sredstava i stoga na uživanje tih korisnika njihove slobode izražavanja zajamčene u članku 11. Povelje (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 28.).
- 102 S obzirom na ozbiljnost miješanja u predmetna temeljna prava utvrđenog nacionalnim propisom, koji u svrhu borbe protiv kriminaliteta određuje zadržavanje podataka o prometu i lokaciji, samo borba protiv teških kaznenih djela može opravdati takvu mjeru (vidjeti analogijom, u pogledu Direktive 2006/24, presudu Digital Rights, t. 60.).
- 103 Nadalje, iako učinkovitost borbe protiv teških kaznenih djela, a osobito protiv organiziranog kriminala i terorizma, može u velikoj mjeri ovisiti o primjeni modernih istražnih tehnika, takav cilj u općem interesu, koliko god bio temeljan, ne može sâm opravdati da se nacionalni propis koji određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji smatra nužnim u svrhu navedene borbe (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 51.).
- 104 U tom pogledu, s jedne strane, valja navesti da je učinak takvog propisa, s obzirom na njegove značajke opisane u točki 97. ove presude, to da je zadržavanje podataka o prometu i lokaciji pravilo, iako sustav uspostavljen Direktivom 2002/58 zahtijeva da to zadržavanje podataka bude iznimka.
- 105 S druge strane, nacionalni propis poput onoga u glavnom postupku, koji na općenit način obuhvaća sve pretplatnike i registrirane korisnike te se odnosi na sva sredstva elektroničke komunikacije kao i na sve podatke o prometu, ne predviđa nikakvo razlikovanje, ograničenje ili iznimku s obzirom na cilj koji se

želi postići. On se općenito odnosi na sve osobe koje se koriste elektroničkim komunikacijskim uslugama a da se pritom te osobe ne nalaze, čak ni posredno, u situaciji koja može dovesti do kaznenih progona. On se, dakle, primjenjuje 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 teškim kaznenim djelima. Nadalje, on ne predviđa nikakvu iznimku pa se primjenjuje i na osobe čije su komunikacije prema pravilima nacionalnog prava podvrgnute profesionalnoj tajni (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 57. i 58.).

- 106 Takav propis ne zahtijeva nikakav odnos između podataka čije je zadržavanje propisano i prijetnje javnoj sigurnosti. Posebice, on nije ograničen na zadržavanje podataka iz jednog privremenog razdoblja i/ili jednog određenog zemljopisnog područja i/ili jednog kruga osoba koje mogu na bilo koji način biti umiješane u teško kazneno djelo ili na osobe koje, ako se zadrže njihovi podaci, mogu zbog drugih razloga doprinijeti borbi protiv kriminaliteta (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 59.).
- 107 Nacionalni propis poput onoga u glavnom postupku prelazi, dakle, granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu, kao što to zahtijeva članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje.
- 108 Nasuprot tomu, članku 15. stavku 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje, ne protivi se to da država članica donese propis koji s ciljem prevencije omogućava ciljano zadržavanje podataka o prometu i lokaciji u svrhu borbe protiv teških kaznenih djela, pod uvjetom da zadržavanje podataka – kad je riječ o kategorijama podataka koji trebaju biti zadržani, predviđenim komunikacijskim sredstvima, osobama na koje se zadržavanje odnosi kao i njegovu trajanju – bude ograničeno na ono što je strogo nužno.
- 109 Kako bi bili ispunjeni zahtjevi određeni u prethodnoj točki ove presude, taj nacionalni propis mora, kao prvo, odrediti jasna i precizna pravila kojima se uređuje doseg i primjena takve mjere zadržavanja podataka te propisati minimalne uvjete, na način da osobe čiji su podaci zadržani raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih osobnih podataka od rizika zlouporabe. On mora osobito naznačiti u kojim okolnostima i pod kojim uvjetima mjera zadržavanja podataka može biti preventivno donesena, jamčeći njezino ograničavanje na ono što je strogo nužno (vidjeti analogijom, u pogledu Direktive 2006/24, presudu Digital Rights, t. 54. i navedenu sudsku praksu).
- 110 Kao drugo, kad je riječ o materijalnim uvjetima koje mora ispuniti nacionalni propis koji u okviru borbe protiv kriminaliteta omogućuje preventivno zadržavanje podataka o prometu i lokaciji, kako bi se osiguralo da to zadržavanje bude ograničeno na ono što je strogo nužno, valja navesti da, iako se takvi uvjeti mogu razlikovati ovisno o mjerama donesenima s ciljem sprečavanja, istrage, otkrivanja i progona teških kaznenih djela, zadržavanje podataka ipak mora nastaviti ispunjavati objektivne kriterije, uspostavljajući vezu između podataka koje treba zadržati i cilja koji se nastoji postići. Navedeni uvjeti moraju se u praksi pokazati takvima da mogu učinkovito ograničiti doseg mjere i stoga javnosti na koju se ona odnosi.
- 111 Kad je riječ o ograničenju takve mjere u pogledu javnosti i okolnosti na koje se ona potencijalno odnosi, nacionalni propis mora se temeljiti na objektivnim kriterijima koji omogućuju obuhvaćanje javnosti čiji podaci mogu otkriti vezu, makar i posrednu, s teškim kaznenim djelima, doprinošenje na bilo koji način borbi protiv teških kaznenih djela ili sprečavanje ozbiljne opasnosti za javnu sigurnost. Takvo ograničenje može se osigurati na temelju zemljopisnog kriterija kad nadležna nacionalna tijela na temelju objektivnih elemenata utvrde da na jednom ili više zemljopisnih područja postoji pojačana opasnost od pripremanja ili počinjenja takvih djela.



- 112 S obzirom na sva prethodna razmatranja, na prvo pitanje u predmetu C-203/15 valja odgovoriti tako da članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje, treba tumačiti na način da mu se protivi nacionalni propis poput onoga u glavnom postupku, koji u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije.

*Drugo pitanje u predmetu C-203/15 i prvo pitanje u predmetu C-698/15*

- 113 Najprije valja navesti da je Kammarrätten i Stockholm (Upravni žalbeni sud u Stockholmu) drugo pitanje u predmetu C-203/15 postavio samo u slučaju niječnog odgovora na prvo pitanje u navedenom predmetu. To drugo pitanje, međutim, ne ovisi o tome ima li zadržavanje podataka opći ili ciljani karakter, kako je predviđeno u točkama 108. do 111. ove presude. Stoga valja zajedno odgovoriti na drugo pitanje u predmetu C-203/15 i prvo pitanje u predmetu C-698/15, koje je postavljeno neovisno o doseg u obveze zadržavanja podataka određene pružateljima elektroničkih komunikacijskih usluga.
- 114 Drugim pitanjem u predmetu C-203/15 i prvim pitanjem u predmetu C-698/15 sudovi koji su uputili zahtjeve u biti pitaju treba li članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7. i 8. i člankom 52. stavkom 1. Povelje, tumačiti na način da mu se protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima a da svrha tog pristupa nije ograničena na borbu protiv teških kaznenih djela, da se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela te da se ne zahtijeva da predmetni podaci budu zadržani na području Unije.
- 115 Kad je riječ o ciljevima koji mogu opravdati nacionalni propis kojim se odstupa od načela povjerljivosti elektroničkih komunikacija, valja podsjetiti da, u mjeri u kojoj je, kako je to utvrđeno u točkama 90. i 102. ove presude, nabranje ciljeva u prvoj rečenici članka 15. stavka 1. Direktive 2002/58 iscrpnog karaktera, pristup zadržanim podacima mora učinkovito i strogo ispunjavati jedan od tih ciljeva. Nadalje, budući da cilj tog propisa mora biti u vezi s ozbiljnošću miješanja u temeljna prava koje uzrokuje taj pristup, slijedi da u području sprečavanja, istrage, otkrivanja i progona kaznenih djela samo borba protiv teških kaznenih djela može opravdati takav pristup zadržanim podacima.
- 116 Kad je riječ o poštovanju načela proporcionalnosti, nacionalni propis koji uređuje uvjete pod kojima pružatelji elektroničkih komunikacijskih usluga moraju nadležnim nacionalnim tijelima odobriti pristup zadržanim podacima, u skladu s onim što je utvrđeno u točkama 95. i 96. ove presude, mora osigurati da do takvog pristupa dođe samo u granicama onoga što je strogo nužno.
- 117 Nadalje, budući da zakonske mjere iz članka 15. stavka 1. Direktive 2002/58, u skladu s njezinom uvodnom izjavom 11., trebaju biti „podložne prikladnim zaštitnim mehanizmima”, takva mjera, kao što to proizlazi iz sudske prakse navedene u točki 109. ove presude, mora propisati jasna i precizna pravila kojima se naznačuje u kojim okolnostima i pod kojim uvjetima pružatelji elektroničkih komunikacijskih usluga trebaju nadležnim nacionalnim tijelima odobriti pristup podacima. Također, takva mjera mora biti zakonski obvezujuća u unutarnjem pravu.
- 118 Kako bi se osiguralo da pristup nadležnih nacionalnih tijela zadržanim podacima bude ograničen na ono što je strogo nužno, na nacionalnom je pravu da utvrdi uvjete pod kojima pružatelji elektroničkih komunikacijskih usluga moraju odobriti takav pristup. Ipak, predmetni nacionalni propis ne može se ograničiti na zahtjev da pristup odgovara jednom od ciljeva iz članka 15. stavka 1. Direktive 2002/58, čak i ako je taj cilj borba protiv teških kaznenih djela. Takav nacionalni propis također mora predvidjeti materijalne i postupovne uvjete kojima se uređuje pristup nadležnih nacionalnih tijela zadržanim podacima (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 61.).

- 119 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, predmetni nacionalni propis mora se temeljiti na objektivnim kriterijima kako bi definirao okolnosti i uvjete u kojima nadležnim nacionalnim tijelima treba biti odobren pristup podacima pretplatnika ili registriranih korisnika. U tom pogledu, pristup u načelu može biti odobren, s obzirom na cilj borbe protiv kriminaliteta, samo podacima osoba za koje postoji sumnja da namjeravaju počinuti ili su počinile teško kazneno djelo ili da su na kakav drugi način sudjelovale u tom djelu (vidjeti analogijom presudu ESLJP-a od 4. prosinca 2015., Zakharov protiv Rusije, CE:ECHR:2015:1204JUD004714306, t. 260.). Ipak, u posebnim okolnostima, poput onih u kojima terorističke aktivnosti predstavljaju prijetnju za vitalne interese nacionalne sigurnosti, obrane ili javne sigurnosti, pristup podacima drugih osoba može se također odobriti kad postoje objektivni elementi koji omogućavaju zaključak da ti podaci u konkretnom slučaju mogu dati stvaran doprinos borbi protiv takvih aktivnosti.
- 120 U svrhu osiguranja punog poštovanja tih uvjeta u praksi, bitno je da pristup nadležnih nacionalnih tijela zadržanim podacima u načelu, osim u valjano opravdanim hitnim slučajevima, bude podvrgnut prethodnom nadzoru suda ili neovisnog upravnog tijela i da odluka tog suda ili tijela bude donesena nakon obrazloženog zahtjeva nacionalnih tijela podnesenog osobito u okviru postupaka sprečavanja, otkrivanja ili progona kaznenih djela (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 62.; vidjeti također analogijom, kad je riječ o članku 8. EKLJP-a, presudu ESLJP-a od 12. siječnja 2016., Szabó i Vissy protiv Mađarske, CE:ECHR:2016:0112JUD003713814, t. 77. i 80.).
- 121 Također, važno je da nadležna nacionalna tijela kojima je odobren pristup zadržanim podacima o tome obavijeste predmetne osobe, u okviru primjenjivih nacionalnih postupaka, čim takva obavijest ne može ugroziti istragu koju vode ta tijela. Ta je informacija zapravo potrebna kako bi im omogućila, među ostalim, ostvarivanje prava na pravni lijek, izričito propisanog člankom 15. stavkom 2. Direktive 2002/58, u vezi s člankom 22. Direktive 95/46, u slučaju povrede njihovih prava (vidjeti analogijom presude od 7. svibnja 2009., Rijkeboer, C-553/07, EU:C:2009:293, t. 52. i od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 95.).
- 122 Kad je riječ o pravilima o sigurnosti i zaštiti podataka koje su zadržali pružatelji elektroničkih komunikacijskih usluga, valja utvrditi da članak 15. stavak 1. Direktive 2002/58 državama članicama ne omogućava odstupanje od članka 4. stavka 1. kao ni od članka 4. stavka 1.b te direktive. Potonje odredbe zahtijevaju da ti pružatelji poduzmu prikladne tehničke i organizacijske mjere koje osiguravaju učinkovitu zaštitu zadržanih podataka od rizika zlouporabe kao i od svakog nezakonitog pristupa tim podacima. Kad je riječ o količini zadržanih podataka, njihovu osjetljivom karakteru i riziku od nezakonitog pristupa tim podacima, pružatelji elektroničkih komunikacijskih usluga moraju prikladnim tehničkim i organizacijskim mjerama, u svrhu osiguranja punog integriteta i povjerljivosti navedenih podataka, jamčiti osobito visoku razinu zaštite i sigurnosti. Nacionalni propis mora osobito propisati zadržavanje na području Unije kao i nepovratno uništenje podataka nakon isteka razdoblja njihova zadržavanja (vidjeti analogijom, kad je riječ o Direktivi 2006/24, presudu Digital Rights, t. 66. do 68.).
- 123 U svakom slučaju, države članice moraju osigurati nadzor od neovisnog tijela poštovanja razine zaštite koju fizičkim osobama jamči pravo Unije kad je riječ o obradi osobnih podataka, s obzirom na to da se takav nadzor izričito zahtijeva člankom 8. stavkom 3. Povelje i, u skladu s ustaljenom sudskom praksom Suda, predstavlja bitan element poštovanja zaštite osoba u odnosu na obradu osobnih podataka. U protivnom bi osobama čiji su osobni podaci zadržani bilo oduzeto pravo zajamčeno u članku 8. stavcima 1. i 3. Povelje na podnošenje zahtjeva za zaštitu njihovih podataka nacionalnim nadzornim tijelima (vidjeti analogijom presudu Digital Rights, t. 68. i presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 41. i 58.).

- 124 Na sudovima koji su uputili zahtjeve jest da provjere poštuju li i u kojoj mjeri nacionalni propisi iz glavnog postupka zahtjeve koji proizlaze iz članka 15. stavka 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje, kako je to istaknuto u točkama 115. do 123. ove presude, kad je riječ kako o pristupu nadležnih nacionalnih tijela zadržanim podacima tako i o zaštiti i razini sigurnosti tih podataka.
- 125 S obzirom na sva prethodna razmatranja, na drugo pitanje u predmetu C-203/15 i na prvo pitanje u predmetu C-698/15 valja odgovoriti tako da članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje, treba tumačiti na način da mu se protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela i kad nije propisano da se predmetni podaci zadržavaju na području Unije.
- Drugo pitanje u predmetu C-698/15*
- 126 Drugim pitanjem u predmetu C-698/15 Court of Appeal (England & Wales) (Civil division) (Žalbeni sud (Engleska i Wales) (Građanski odjel)) u biti pita je li u presudi Digital Rights Sud protumačio članke 7. i 8. Povelje u širem smislu od onoga koji je Europski sud za ljudska prava pridao članku 8. EKLJP-a.
- 127 Najprije valja navesti da, iako su, kao što to potvrđuje članak 6. stavak 3. UEU-a, temeljna prava priznata EKLJP-om dio prava Unije kao opća načela, navedena konvencija, sve dok Unija nije njezina stranka, ne čini pravni instrument koji je formalno integriran u pravni poredak Unije (vidjeti u tom smislu presudu od 15. veljače 2016., N., C-601/15 PPU, EU:C:2016:84, t. 45. i navedenu sudsku praksu).
- 128 Stoga tumačenje Direktive 2002/58, o kojoj je riječ u ovom predmetu, mora biti izvršeno samo s obzirom na temeljna prava zajamčena Poveljom (vidjeti u tom smislu presudu od 15. veljače 2016., N., C-601/15 PPU, EU:C:2016:84, t. 46. i navedenu sudsku praksu).
- 129 Nadalje, valja istaknuti da objašnjenja koja se odnose na članak 52. Povelje navode da je cilj stavka 3. tog članka osiguranje potrebne sukladnosti između Povelje i EKLJP-a, „bez štetnog učinka na autonomiju prava Unije i Suda Europske unije” (presuda od 15. veljače 2016., N., C-601/15 PPU, EU:C:2016:84, t. 47.). Osobito, kao što je to izričito određeno drugom rečenicom članka 52. stavka 3. Povelje, prva rečenica u toj odredbi ne omogućava da pravo Unije pruži širu zaštitu od one koju pruža EKLJP. Tomu naposljetku valja dodati da se članak 8. Povelje odnosi na temeljno pravo koje se razlikuje od onoga iz članka 7. Povelje te u odnosu na koje ne postoji ekvivalentno pravo u EKLJP-u.
- 130 Prema ustaljenoj sudskoj praksi Suda, opravdanost zahtjeva za prethodnu odluku nije u davanju savjetodavnih mišljenja o općenitim ili hipotetskim pitanjima, nego u stvarnoj potrebi učinkovitog rješenja spora o pravu Unije (vidjeti u tom smislu presude od 24. travnja 2012., Kamberaj, C-571/10, EU:C:2012:233, t. 41.; od 26. veljače 2013., Åkerberg Fransson, C-617/10, EU:C:2013:105, t. 42. i od 27. veljače 2014., Pohotovost, C-470/12, EU:C:2014:101, t. 29.).
- 131 U predmetnom slučaju, s obzirom na razmatranja koja se nalaze, među ostalim, u točkama 128. i 129. ove presude, pitanje prelazi li zaštita određena u člancima 7. i 8. Povelje onu koja je zajamčena člankom 8. EKLJP-a ne može utjecati na tumačenje Direktive 2002/58 koje je dano u vezi s Poveljom i u glavnom postupku u predmetu C-698/15.
- 132 Stoga se ne čini da odgovor na drugo pitanje u predmetu C-698/15 može pružiti elemente za tumačenje prava Unije koji bi bili nužni za rješavanje navedenog spora s obzirom na to pravo.

133 Iz toga slijedi da je drugo pitanje u predmetu C-698/15 nedopušteno.

### **Troškovi**

134 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 navedenoga, Sud (veliko vijeće) odlučuje:

1. **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 člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da mu se protivi nacionalni propis poput onoga u glavnom postupku, koji u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije.**
2. **Članak 15. stavak 1. Direktive 2002/58, kako je izmijenjena Direktivom 2009/136, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje o temeljnim pravima, treba tumačiti na način da mu se protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela i kad nije propisano da se predmetni podaci zadržavaju na području Unije.**
3. **Drugo pitanje koje je uputio Court of Appeal (England & Wales) (Civil Division) (Žalbeni sud (Engleska i Wales) (Građanski odjel), Ujedinjena Kraljevina) je nedopušteno.**

Potpisi