Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 21. decembra 2016*

„Predhodno odločanje — Elektronske komunikacije — Obdelava osebnih podatkov — Zaupnost elektronskih komunikacij — Varstvo — Direktiva 2002/58/ES — Členi 5, 6, 9 in 15(1) — Listina Evropske unije o temeljnih pravicah — Členi 7, 8, 11 in 52(1) — Nacionalna zakonodaja — Ponudniki elektronskih komunikacijskih storitev — Obveznost splošne in neselektivne hrambe podatkov o prometu in o lokaciji — Nacionalni organi — Dostop do podatkov — Neobstoj predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa — Skladnost s pravom Unije“

V združenih zadevah C-203/15 in C-698/15,

katerih predmet sta predloga za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki sta ga vložili Kammarrätten i Stockholm (pritožbeno upravno sodišče v Stockholmu, Švedska) in Court of Appeal (England & Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek), Združeno kraljestvo) z odločbama z dne 29. aprila 2015 in z dne 9. decembra 2015, ki sta na Sodišče prispeli 4. maja 2015 in 28. decembra 2015, v postopkih

Tele2 Sverige AB (C-203/15)

proti

Post- och telestyrelsen,

in

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

proti

Tomu Watsonu,

Petru Briceu,

Geoffreyju Lewisu,

ob udeležbi

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

* Jezika postopka: švedščina in angleščina.

SODIŠČE (veliki senat),

v sestavi K. Lenaerts, predsednik, A. Tizzano, podpredsednik, R. Silva de Lapuerta, predsednica senata, T. von Danwitz (poročevalec), J. L. da Cruz Vilaça, E. Juhász in M. Vilaras, predsedniki senatov, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen in C. Lycourgos, sodniki,

generalni pravobranilec: H. Saugmandsgaard Øe,

sodna tajnica: C. Strömholm, administratorka,

na podlagi sklepa predsednika Sodišča z dne 1. februarja 2016, da se zadeva C-698/15 obravnava po hitrem postopku v skladu s členom 105(1) Poslovnika Sodišča,

na podlagi pisnega postopka in obravnave z dne 12. aprila 2016,

ob upoštevanju stališč, ki so jih predložili:

— za Tele2 Sverige AB M. Johansson in N. Torgerzon, odvetnika, ter E. Lagerlöf in S. Backman,

— za T.Watsona J. Welch, E. Norton, solicitors, I. Steele, odvetnik, B. Jaffey, barrister, in D. Rose, QC,

— za P. Bricea in G. Lewisa A. Suterwalla in R. de Mello, barristers, R. Drabble, QC, in S. Luke, solicitor,

— za Open Rights Group in Privacy International D. Carey, solicitor, R. Mehta in J. Simor, barristers,

— za The Law Society of England and Wales T. Hickman, barrister, in N. Turner,

— za švedsko vlado A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren in L. Swedenborg, agenti,

— za vlado Združenega kraljestva S. Brandon, L. Christie in V. Kaye, agenti, skupaj z D. Beardom, G. Facenno, J. Eadiejem, QC, in S. Ford, barrister,

— za belgijsko vlado J.-C. Halleux, S. Vanrie in C. Pochet, agenti,

— za češko vlado M. Smolek in J. Vláčil, agenta,

— za dansko vlado C. Thorning in M. Wolff, agenta,

— za nemško vlado T. Henze, M. Hellmann in J. Kemper, agenti, skupaj z M. Kottmannom in U. Karpensteinom, odvetnikoma,

— za estonsko vlado K. Kraavi-Käerdi, agentka,

— za Irsko E. Creedon, L. Williams in A. Joyce, agenti, skupaj z D. Fennellyjem, BL,

— za špansko vlado A. Rubio González, agent,

— za francosko vlado G. de Bergues, D. Colas, F.-X. Bréchot in C. David, agenti,

— za ciprsko vlado K. Kleanthous, agentka,

— za madžarsko vlado M. Fehér in G. Koós, agenta,

— za nizozemsko vlado M. Bulterman, M. Gijzen in J. Langer, agenti,

— za poljsko vlado B. Majczyna, agent,

— za finsko vlado J. Heliskoski, agent,

— za Evropsko komisijo H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira in J. Vondung, agenti,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 19. julija 2016

izreka naslednjo

Sodbo

1 Predloga za sprejetje prehodne odločbe se nanašata na razlago člena 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11) (v nadaljevanju: Direktiva 2002/58) glede na člene 7, 8 in 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).

2 Ta predloga sta bila vložena v okviru dveh sporov, prvič, med Tele2 Sverige AB in Post- och telestyrelsen (švedski regulativni organ za pošto in telekomunikacije, v nadaljevanju: PTS) glede odredbe zadnjenavedenega, naslovljene na Tele2 Sverige, da hrani podatke o prometu in podatke o lokaciji svojih naročnikov in registriranih uporabnikov (zadeva C-203/15), in, drugič, med Tomom Watsonom, Petrom Briceom in Geoffreyjem Lewisom ter Secretary of State for the Home Department (ministrstvo za notranje zadeve, Združeno kraljestvo Velika Britanija in Severna Irska) glede skladnosti člena 1 Data Retention and Investigatory Powers Act 2014 (zakon o hrambi podatkov in preiskovalnih pooblastilih iz leta 2014, v nadaljevanju: DRIPA) s pravom Unije (zadeva C-698/15).

Pravni okvir

Pravo Unije

Direktiva 2002/58

3 V uvodnih izjavah 2, 6, 7, 11, 21, 22, 26 in 30 Direktive 2002/58 je navedeno:

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

[…]

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

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

[…]

(11) Ta direktiva, tako kot Direktiva [Evropskega parlamenta in Sveta] 95/46/ES [z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355)] ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red Skupnosti. Zato ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito javne varnosti, obrambe, državne varnosti (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve državne varnosti) in izvajanje kazenske zakonodaje. Ta direktiva torej ne vpliva na zmožnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so potrebni iz katerega koli od teh namenov ter v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, kakor jo razlaga Evropsko sodišče za človekove pravice v svojih sodbah. Taki ukrepi morajo biti ustrezni, dosledno sorazmerni z namenom in potrebni v demokratični družbi ter predmet primernih zaščitnih ukrepov v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.

[…]

(21) Za zagotovitev zaupnosti sporočil, vključno z njihovo vsebino in vsemi podatki glede teh sporočil, je treba sprejeti ukrepe za preprečitev nedovoljenega dostopa do sporočil, poslanih prek javnih komunikacijskih omrežij in javno dostopnih elektronskih komunikacijskih storitev. Nacionalna zakonodaja v nekaterih državah članicah prepoveduje le nameren nedovoljen dostop do sporočil.

(22) Prepoved shranjevanja sporočil in s tem povezanih podatkov o prometu osebam, ki niso uporabniki ali ki nimajo privolitve uporabnikov, ni namenjena prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa v omrežju elektronskih komunikacij in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena v času njihovega hranjenja. […]

[…]

(26) Podatki o naročnikih, ki se obdelajo v elektronskih komunikacijskih omrežjih zaradi vzpostavitve povezav in prenosa podatkov, vsebujejo podatke o zasebnem življenju fizičnih oseb in zadevajo pravico do spoštovanja njihove korespondence ali legitimne interese pravnih oseb. Takšni podatki se lahko shranijo le v obsegu, potrebnem za izvedbo storitve, za namen zaračunavanja in plačila medsebojnih povezav ter za določen čas. Vsaka nadaljnja obdelava takih podatkov […] je dovoljena samo takrat, kadar naročnik v to privoli na podlagi točnih in popolnih podatkov, ki jih dobi od ponudnika javno razpoložljivih elektronskih komunikacijskih storitev o vrsti nadaljnje obdelave, ki jo ta namerava izvajati, in o naročnikovi pravici, da ne da privolitve za tako obdelavo ali da jo umakne. […]

[…]

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

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

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

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

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

5 Člen 2 Direktive 2002/58, naslovljen „Opredelitve“, določa:

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

Uporabijo se tudi naslednje opredelitve pojmov:

[…]

(b) ‚podatki o prometu‘ pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila;

(c) ‚podatki o lokaciji‘ pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve;

(d) ‚sporočilo‘ (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve. To ne vključuje nobenih podatkov, prenesenih javnosti kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da podatek povezati s prepoznavnim naročnikom ali uporabnikom, ki ga prejme;

[…]“

6 Člen 3 Direktive 2002/58, naslovljen „Storitve“, določa:

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

7 Člen 4 te direktive, naslovljen „Varnost obdelave“, določa:

„1. Ponudnik javno razpoložljive elektronske komunikacijske storitve mora sprejeti ustrezne tehnične in organizacijske ukrepe, da zagotovi varnost svojih storitev, če je treba skupaj s ponudnikom javnega komunikacijskega omrežja, kar zadeva varnost omrežja. Ob upoštevanju stanja tehnike in stroškov za izvedbo, morajo ti ukrepi zagotoviti raven varnosti, ki ustreza predvidenemu tveganju.

1a. Brez poseganja v Direktivo [95/46], ukrepi iz odstavka 1 najmanj:

— zagotavljajo, da ima dostop do osebnih podatkov le pooblaščeno osebje za z zakonom dovoljene namene,

— varujejo shranjene ali poslane osebne podatke pred nenamernim ali nezakonitim uničenjem, nenamerno izgubo ali spremembo ter nepooblaščeno ali nezakonito hrambo, obdelavo, dostopom ali razkritjem, in

— zagotavljajo izvajanje varnostne politike pri obdelavi osebnih podatkov.

[…]“

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

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

[…]

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

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

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

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

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

[…]

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

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

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

11 Člen 15 te direktive, naslovljen „Uporaba nekaterih določb Direktive [95/46]“, določa:

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

[…]

1b. Ponudniki morajo vzpostaviti notranje postopke za odzivanje na zahteve za dostop do osebnih podatkov uporabnikov, ki temeljijo na nacionalnih določbah, sprejetih v skladu z odstavkom 1. Pristojnim nacionalnim organom morajo, na njihovo zahtevo, predložiti informacije o teh postopkih, število prejetih zahtevkov, sklicevanje na pravno utemeljitev in njihov odgovor.

2. Določbe poglavja III o pravnih sredstvih, odgovornosti in sankcijah Direktive [95/46] se uporabijo v zvezi z nacionalnimi predpisi, sprejetimi v skladu s to direktivo in posameznimi pravicami, izhajajočimi iz te direktive.

[…]“

Direktiva 95/46

12 Člen 22 Direktive 95/46 iz poglavja III te direktive določa:

„Brez poseganja v upravnopravna pravna sredstva pred predložitvijo zadeve sodnemu organu, ki jih je možno med drugim predvideti pred nadzornim organom iz člena 28, države članice zagotovijo, da ima vsaka oseba v primeru kršitve pravic, zagotovljenih z nacionalno zakonodajo, ki se nanaša na zadevno obdelavo, pravico vložiti pravno sredstvo na sodišču.“

Direktiva 2006/24/ES

13 Člen 1 Direktive 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL 2006, L 105, str. 54), naslovljen „Predmet urejanja in področje uporabe“, v odstavku 2 določa:

„Ta direktiva se uporablja za podatke o prometu in lokaciji pravnih subjektov in fizičnih oseb, kakor tudi za povezane podatke, potrebne za določitev naročnika ali registriranega uporabnika. Ne uporablja se za vsebino elektronskih komunikacij, vključno z informacijami, pregledanimi z uporabo elektronskega komunikacijskega omrežja.“

14 Člen 3 te direktive, naslovljen „Obveznost hrambe podatkov“, določa:

„1. Z odstopanjem od členov 5, 6 in 9 Direktive [2002/58] države članice sprejmejo ukrepe za zagotovitev, da so podatki, opredeljeni v členu 5 te direktive, hranjeni v skladu z določbami te direktive, kolikor se pridobivajo ali obdelujejo pri ponudnikih javno dostopnih elektronskih komunikacijskih storitev ali javnega komunikacijskega omrežja v njihovi pristojnosti v procesu zagotavljanja zadevnih komunikacijskih storitev.

2. Obveznost hrambe podatkov iz odstavka 1 vključuje hrambo podatkov, kakor je določena v členu 5 glede neuspešnih klicev, kjer se podatki pridobivajo ali obdelujejo in hranijo (pri podatkih o telefoniji) ali beležijo (pri internetnih podatkih) pri ponudnikih javno dostopnih elektronskih komunikacijskih storitev ali javnega komunikacijskega omrežja v pristojnosti zadevnih držav članic v procesu zagotavljanja zadevnih komunikacijskih storitev. Ta direktiva ne zahteva hrambe podatkov o neuspešnih povezavah.“

Švedsko pravo

15 Iz predložitvene odločbe v zadevi C-203/15 izhaja, da je švedski zakonodajalec zaradi prenosa Direktive 2006/24 v nacionalno pravo spremenil Lagen (2003:389) om elektronisk kommunikation (zakon 2003:389 o elektronskih komunikacijah, v nadaljevanju: LEK) in Förordningen (2003:396) om elektronisk kommunikation (uredba št. 2003:396 o elektronskih komunikacijah). Besedili, v različicah, ki sta se uporabljali v postopku v glavni stvari, vsebujeta pravila o hrambi podatkov v zvezi z elektronskimi komunikacijami in pravila o dostopu nacionalnih organov do teh podatkov.

16 Dostop do teh podatkov urejata tudi Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (zakon 2012:278 o sporočanju podatkov o elektronskih komunikacijah v okviru preiskovalnih dejavnosti organov pregona, v nadaljevanju: zakon 2012:278) in Rättegångsbalken (zakonik o sodnem postopku, v nadaljevanju: RB).

Obveznost hrambe podatkov v zvezi z elektronskimi komunikacijami

17 V skladu z navedbami predložitvenega sodišča v zadevi C-203/15 določbe člena 16a poglavja 6 LEK v povezavi s členom 1 poglavja 2 tega zakona določajo, da morajo ponudniki elektronskih komunikacijskih storitev hraniti podatke, katerih hrambo določa Direktiva 2006/24. Obveznost hrambe zajema naročniške podatke in vse druge podatke o elektronskih komunikacijah, ki so potrebni za sledenje in prepoznanje vira komunikacije, cilja komunikacije, datuma, časa in trajanja komunikacije, vrste komunikacije, komunikacijske opreme in lokacije komunikacijske opreme na začetku in koncu komunikacije. Obveznost hrambe podatkov zajema podatke, pridobljene ali obdelane v okviru telefonskih storitev, telefonskih storitev, ki uporabljajo mobilno povezavo, prenosa elektronskih

sporočil, storitev internetnega dostopa in zagotavljanja kapacitete internetnega dostopa (oblika dostopa). Ta obveznost velja tudi za podatke o neuspešnih komunikacijah. Ne zajema pa vsebine komunikacij.

18 Členi od 38 do 43 uredbe št. 2003:396 o elektronskih komunikacijah podrobno določajo vrste podatkov, ki jih je treba hraniti. Pri telefonskih storitvah morajo podatki, ki jih je treba hraniti, obsegati kličočo in klicano številko ter datum in sledljiv čas začetka in konca komunikacije. Za telefonske storitve, ki uporabljajo mobilno povezavo, veljajo dodatne zahteve, tako da je treba na primer hraniti tudi podatke o lokaciji začetka in konca komunikacije. Za telefonske storitve, ki obsegajo pakete IP, morajo podatki, ki jih je treba hraniti, poleg gornjega vsebovati IP naslova kličoče in klicane osebe. Podatki, ki jih je treba hraniti o storitvah prenosa elektronskih sporočil, obsegajo številko pošiljatelja in prejemnika, IP naslove ali vse druge naslove za sprejemanje sporočil. Pri dostopu do interneta je treba hraniti na primer podatke v zvezi z IP naslovi uporabnikov ter datum in sledljiv čas prijave in odjave storitve, ki zagotavlja dostop do interneta.

Trajanje hrambe podatkov

19 V skladu s členom 16d poglavja 6 LEK morajo ponudniki elektronskih komunikacijskih storitev podatke iz člena 16a tega poglavja hraniti šest mesecev od dneva konca komunikacije. Nato je treba podatke nemudoma uničiti, če člen 16d, drugi odstavek, ne določa drugače.

Dostop do hranjenih podatkov

20 Dostop nacionalnih organov do hranjenih podatkov urejajo določbe zakona 2012:278, LEK in RB.

– Zakon 2012:278

21 V okviru preiskovalnih dejavnosti lahko v skladu s členom 1 zakona 2012:278 nacionalna policija, Säkerhetspolisen (obveščevalna služba, Švedska) in Tullverket (carinska uprava, Švedska) pod pogoji, določenimi s tem zakonom, brez vednosti ponudnika elektronskega komunikacijskega omrežja ali elektronskih komunikacijskih storitev, ki so dovoljene na podlagi LEK, zbirajo podatke o sporočilih, poslanih v omrežju elektronskih komunikacij, o elektronski komunikacijski opremi, prisotni na določenem geografskem območju, in o geografskih območjih, na katerih je ali je bila locirana elektronska komunikacijska oprema.

22 V skladu s členoma 2 in 3 zakona 2012:278 se smejo podatki načeloma zbirati, če so okoliščine take, da je ukrep posebej pomemben za preprečitev, odvrnitev ali odkritje kriminalne dejavnosti, ki obsega eno ali več kaznivih dejanj, za katera je predpisana kazen zapora najmanj dve leti, ali kazniva dejanja, našteta v členu 3 tega zakona, vključno s kaznivimi dejanji, za katera je določena kazen zapora manj kot dve leti. Razlogi, zaradi katerih se zahteva ukrep, morajo prevladati nad posegom v pravice ali drugo škodo, ki jo ukrep povzroči osebam, proti katerim je uperjen, ali interesu, ki mu nasprotuje. V skladu s členom 5 tega zakona ukrep ne sme trajati več kot en mesec.

23 Odločbo o tem ukrepu sprejme predstojnik zadevnega organa ali uslužbenec, na katerega je bilo preneseno pooblastilo za odločanje. Za to vrsto ukrepa ni potreben predhodni nadzor sodnega organa ali neodvisnega upravnega organa.

24 Na podlagi člena 6 zakona 2012:278 mora biti Säkerhets och integritetsskyddsnämnden (komisija za varovanje varnosti in integritete, Švedska) obveščena o vsakršni odločbi o dovoljenju za zbiranje podatkov. V skladu s členom 1 Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (zakon 2007:980 o nadzoru nekaterih dejavnosti pregona) mora ta komisija nadzirati, kako organi pregona uporabljajo zakon.

– LEK

25 V skladu s členom 22, prvi odstavek, točka 2, poglavja 6 LEK mora vsak ponudnik elektronskih komunikacijskih storitev na zahtevo predati naročniške podatke tožilstvu, nacionalni policiji, obveščevalni službi ali kateremu koli drugemu javnemu organu pregona, če se navedeni podatki nanašajo na domnevno storjeno kaznivo dejanje. Na podlagi navedb predložitvenega sodišča v zadevi C-203/15 ni nujno, da gre za hudo kaznivo dejanje.

– RB

26 RB ureja sporočanje hranjenih podatkov nacionalnim organom v predhodnih preiskavah. V skladu s členom 19 poglavja 27 RB se „nadzor nad elektronskimi komunikacijami“ brez vednosti tretje osebe načeloma dovoli v predhodnih preiskavah, ki se nanašajo na kazniva dejanja, za katera je zagrožena kazen zapora najmanj šest mesecev. Z „nadzorom nad elektronskimi komunikacijami“ je treba v skladu s členom 19 poglavja 27 RB razumeti pridobitev podatkov brez vednosti tretje osebe o sporočilu, poslanemu prek omrežja elektronskih komunikacij, o elektronski komunikacijski opremi, prisotni na določenem geografskem območju, in o geografskih območjih, na katerih je ali je bila locirana elektronska komunikacijska oprema.

27 Po navedbah predložitvenega sodišča v zadevi C-203/15 informacij o vsebini sporočila ni mogoče pridobiti na podlagi člena 19 poglavja 27 RB. Praviloma se sme nadzor nad elektronskimi komunikacijami na podlagi člena 20 poglavja 27 RB odrediti le, če obstajajo utemeljeni razlogi za sum, da je neka oseba storila kaznivo dejanje, ukrep pa je za preiskavo posebej pomemben, ker se nanaša na kaznivo dejanje, za katero je predpisana kazen najmanj dve leti zapora, ali poskus, pripravo ali hudodelsko združevanje za storitev takega kaznivega dejanja. V skladu s členom 21 poglavja 27 RB mora tožilstvo razen v nujnih primerih pristojno sodišče zaprositi za dovoljenje za izvajanje nadzora nad elektronskimi komunikacijami.

Varnost in varstvo hranjenih podatkov

28 V skladu s členom 3a poglavja 6 LEK morajo ponudniki elektronskih komunikacijskih storitev, ki so zavezani za hrambo podatkov, sprejeti posebne tehnične in organizacijske ukrepe, potrebne za varstvo podatkov med obdelavo. Po navedbah predložitvenega sodišča v zadevi C-203/15 pa v švedski zakonodaji ni določb o tem, kje je treba hraniti podatke.

Pravo Združenega kraljestva

DRIPA

29 Razdelek 1 DRIPA, naslovljen „Pooblastila za hrambo upoštevnih podatkov v zvezi s komunikacijami, ki so predmet varstva“, določa:

„(1) [Ministrstvo za notranje zadeve] lahko z odločbo (v nadaljevanju: odločba o hrambi) od javnega telekomunikacijskega operaterja zahteva hrambo upoštevnih podatkov v zvezi s komunikacijami, če meni, da je zahteva nujna in sorazmerna iz enega ali več razlogov, navedenih v točkah od (a) do (h) razdelka 22(2) Regulation of Investigatory Powers Act 2000 (zakon o preiskovalnih pooblastilih iz leta 2000) (nameni, za katere je mogoče pridobiti komunikacijske podatke).

(2) Odločba o hrambi lahko:

(a) velja za določenega operaterja ali kakršno koli kategorijo operaterjev;

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

(c) določi obdobje ali obdobja, v katerih je treba hraniti podatke;

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

(e) uvede različne določbe za različne namene;

(f) zadeva podatke, ki v času izdaje ali začetka veljavnosti odločbe o hrambi obstajajo ali ne obstajajo.

(3) [Ministrstvo za notranje zadeve] lahko s pravilniki sprejme nadaljnje določbe o hrambi upoštevnih komunikacijskih podatkov.

(4) Take določbe lahko zlasti vključujejo opredelitev:

(a) zahtev pred izdajo odločbe o hrambi;

(b) maksimalnega obdobja, v katerem se podatki hranijo na podlagi odločbe o hrambi;

(c) vsebine, izdaje, začetka veljavnosti, pregleda, spremembe ali preklica odločbe o hrambi;

(d) celovitosti, varnosti ali varstva podatkov, hranjenih na podlagi tega razdelka, dostopa do teh podatkov in njihovega razkritja in uničenja;

(e) izvrševanja ustreznih zahtev ali omejitev oziroma preverjanja skladnosti z njimi;

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

(g) povračila stroškov s strani [ministrstva za notranje zadeve] (pod nekaterimi pogoji ali brez), ki so nastali javnim telekomunikacijskim operaterjem zaradi spoštovanja upoštevnih zahtev ali omejitev;

(h) tega, da [(Data Retention (EC Directive) Regulations 2009 (pravilnik iz leta 2009 o hrambi podatkov v smislu direktive ES)] preneha veljati, in prehoda k hrambi podatkov v skladu s tem razdelkom.

(5) Maksimalno obdobje, določeno v skladu z odstavkom (4)(b), ne sme presegati 12 mesecev, šteto od dneva, ki je v zvezi z zadevnimi podatki določen v pravilnikih v skladu z odstavkom (3).

[…]“

30 Razdelek 2 DRIPA določa, da izraz „upoštevni podatki v zvezi s komunikacijami“ pomeni „upoštevne podatke v zvezi s komunikacijami take vrste, kot so navedeni v prilogi k pravilniku iz leta 2009 o hrambi podatkov v skladu z direktive ES, kadar take podatke zbirajo ali obdelajo javni telekomunikacijski operaterji v Združenem kraljestvu v postopku zagotavljanja zadevnih telekomunikacijskih storitev“.

RIPA

31 Razdelek 21 zakona o preiskovalnih pooblastilih iz leta 2000 (v nadaljevanju: RIPA) iz poglavja II tega zakona, naslovljen „Pridobitev in razkritje podatkov v zvezi s komunikacijo“, v odstavku 4 določa:

„V tem poglavju ‚podatki v zvezi s komunikacijami‘ pomenijo kar koli od tega:

(a) podatek o prometu, ki je v komunikaciji ali je tej priložen (s strani pošiljatelja ali kako drugače), za namene vseh poštnih storitev ali telekomunikacijskih sistemov, s katerim se ali se lahko prenaša;

(b) informacijo, ki ne vključuje nobene vsebine komunikacije (razen informacij, ki spadajo pod točko (a)) in ki zadeva uporabo s strani katere koli osebe:
(i) poštne ali telekomunikacijske storitve; ali
(ii) v zvezi z zagotavljanjem ali uporabo telekomunikacijske storitve ali katerega koli dela telekomunikacijskega sistema s strani neke osebe;

(c) informacijo, ki ne spada pod točki (a) ali (b), ki jo v zvezi z osebami, katerim zagotavlja storitev, ima ali jo je pridobila oseba, ki ponuja poštno ali telekomunikacijsko storitev.“

32 V skladu z navedbami iz predložitvene odločbe v zadevi C-698/15 ti podatki vključujejo „podatke o lokaciji uporabnika“, ne vključujejo pa podatkov o vsebini komunikacije.

33 Razdelek 22 RIPA glede dostopa do hranjenih podatkov določa:

„(1) Ta razdelek se uporablja, če odgovorna oseba za namen tega poglavja oceni, da je treba iz razlogov iz odstavka 2 tega razdelka pridobiti vse podatke o komunikaciji.

(2) Pridobitev podatkov v zvezi s komunikacijo je iz razlogov iz tega odstavka nujna, če je to potrebno:

(a) v interesu nacionalne varnosti;

(b) za preprečevanje ali odkrivanje kaznivih dejanj ali preprečevanje kršitev javnega reda;

(c) v interesu gospodarske blaginje Združenega kraljestva;

(d) v interesu javne varnosti;

(e) za varovanje javnega zdravja;

(f) za odmero ali pobiranje davkov, pristojbin, dajatev ali drugih naloženih bremen, prispevkov ali taks, ki jih je treba plačati javni upravi;

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

(h) iz drugih razlogov (ki niso navedeni v točkah od (a) do (g)), opredeljenih v odredbi [ministrstva za notranje zadeve].

(4) Če ni drugače določeno v odstavku 5, lahko odgovorna oseba, če meni, da telekomunikacijski operater ali operater poštnih storitev razpolaga, bi lahko razpolagal ali bi bil zmožen razpolagati s podatki, od tega operaterja z odredbo zahteva, da

(a) pridobi podatke, če z njimi še ne razpolaga, in

(b) v vsakem primeru razkrije vse podatke, s katerimi razpolaga ali ki jih je pridobil kasneje.

(5) Odgovorna oseba izda dovoljenje v skladu z odstavkom 3 ali izda odredbo na podlagi odstavka 4 le, če meni, da pridobitev zadevnih podatkov, ki je posledica dovoljenega ali zahtevanega ravnanja na podlagi dovoljenja ali odredbe, sorazmerna s ciljem pridobitve podatkov.“

34 V skladu z razdelkom 65 RIPA je pritožbo mogoče predložiti pri Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo), če obstaja razlog za bojazen, da so bili podatki pridobljeni neustrezno.

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (pravilnik iz leta 2014 o hrambi podatkov, ki je bil sprejet na podlagi DRIPA, je razdeljen na tri dele, s tem da drugi del obsega člene od 2 do 14 tega pravilnika. Člen 4, naslovljen „Odredbe za hrambo“, določa:

„(1) V odredbah za hrambo je treba navesti:

(a) javnega telekomunikacijskega operaterja (ali opis operaterjev), na katerega so naslovljene,

(b) zadevne podatke v zvezi s komunikacijami, ki jih je treba hraniti,

(c) obdobje ali obdobja, v katerih je treba hraniti podatke,

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

(2) Z odredbo o hrambi podatkov ni mogoče zahtevati, da se podatek hrani za dlje kot 12 mesecev, pri čemer se to obdobje začne:

(a) v primeru podatkov o prometu ali podatkov v zvezi z uporabo storitve z dnem zadevne komunikacije in

(b) v primeru podatkov v zvezi z naročniki z dnem, ko zadevna oseba prekine zadevno komunikacijsko storitev oziroma z dnem, ko se podatek spremeni (če do tega pride prej).

[…]“

36 Člen 7 tega pravilnika, naslovljen „Celovitost in varnost podatkov“, določa:

„(1) Javni telekomunikacijski operater, ki hrani podatke v skladu z razdelkom 1 [DRIPA], mora:

(a) zagotoviti enako celovitost in vsaj enako raven varnosti in varstva podatkov, kot jih imajo podatki v sistemih, iz katerih prihajajo,

(b) z ustreznimi tehničnimi in organizacijskimi ukrepi zagotoviti, da do podatkov lahko dostopa le osebje, ki ima za to posebno dovoljenje, in

(c) z ustreznimi tehničnimi in organizacijskimi ukrepi zavarovati podatke pred nezakonitim uničenjem, nenamerno izgubo ali spremembo oziroma pred nepooblaščeno ali nezakonito hrambo, obdelavo, dostopom ali razkritjem.

(2) Javni telekomunikacijski operater, ki hrani podatke v zvezi s komunikacijami na podlagi člena 1 [DRIPA], mora uničiti podatke, če hramba podatkov ni več dovoljena na podlagi tega člena niti ni drugače zakonsko dovoljena.

(3) Zahteva iz odstavka 2 glede uničenja podatkov pomeni izbris podatkov na način, da dostop do njih ni več mogoč.

(4) Zadostuje, da operater sprejme ukrepe, da se podatki brišejo enkrat na mesec ali pogosteje, glede na možnosti, ki jih ima ta operater v praksi.“

37 Člen 8 tega pravilnika, naslovljen „Razkritje hranjenih podatkov“, določa:

„(1) Javni telekomunikacijski operater mora vzpostaviti ustrezne varnostne sisteme (ki vsebujejo tehnične in organizacijske ukrepe), ki določajo dostop do podatkov v zvezi s komunikacijami, hranjenih na podlagi razdelka 1 [DRIPA], da se prepreči vsako razkritje podatkov, ki ne spadajo v razdelek 1(6)(a) [DRIPA].

(2) Javni telekomunikacijski operater, ki hrani podatke na podlagi razdelka 1 [DRIPA], mora hraniti podatke tako, da jih lahko na zahtevo predloži brez nepotrebnega odlašanja.“

38 Člen 9 tega pravilnika, naslovljen „Nadzor informacijskega pooblaščenca“, določa:

„Informacijski pooblaščenec nadzoruje spoštovanje zahtev ali omejitev, določenih v tem delu, glede celovitosti, varnosti in uničenja podatkov, hranjenih na podlagi člena 1 [DRIPA].“

Kodeks o pridobitvi

39 Acquisition and Disclosure of Communications Data Code of Practice (kodeks ravnanja v zvezi s pridobitvijo in razkritjem podatkov v zvezi s komunikacijami, v nadaljevanju: kodeks o pridobitvi) v točkah od 2.5 do 2.9 in od 2.36 do 2.45 določa smernice v zvezi z nujnostjo in sorazmernostjo pridobitve podatkov v zvezi s komunikacijami. Glede na pojasnila predložitvenega sodišča v zadevi C-698/15 je treba v skladu s točkami od 3.72 do 3.77 tega kodeksa posebno pozornost nameniti nujnosti in sorazmernosti, kadar se zahtevani podatki v zvezi s komunikacijami nanašajo na osebo, ki opravlja poklic, v okviru katerega obravnava informacije, ki so varovani kot poklicna skrivnost, ali druge zaupne informacije.

40 Na podlagi točk od 3.78 do 3.84 tega kodeksa je v posebnem primeru zahteve za podatke v zvezi s komunikacijami, ki se vloži zaradi identifikacije novinarjevega vira, potreben sodni sklep. Na podlagi točk od 3.85 do 3.87 tega kodeksa se, če dostop zahtevajo lokalni organi, zahteva sodna odobritev. Za dostop do podatkov v zvezi s komunikacijami, ki so z zakonom varovane kot zakonska poklicna skrivnost, ali do podatkov v zvezi s komunikacijami, ki se nanašajo na zdravnike, poslance ali duhovnike, pa se, nasprotno, ne zahteva dovoljenje sodišča ali neodvisnega organa.

41 Točka 7.1 kodeksa o pridobitvi določa, da je treba podatke v zvezi s komunikacijami, zahtevane ali pridobljene v skladu z določbami RIPA, ter vse njihove izvlečke, povzetke in kopije obdelovati in hraniti varno. Poleg tega je treba spoštovati zahteve, navedene v Data Protection Act (zakon o varstvu podatkov).

42 Točka 7.18 kodeksa o pridobitvi določa, da kadar javni organ Združenega kraljestva razmišlja o morebitnem razkritju podatkov v zvezi s komunikacijami tujim organom, mora med drugim preučiti, ali bodo ti podatki ustrezno varovani. Vendar točka 7.22 tega kodeksa določa, da se podatke lahko prenese v tretje države – če je ta prenos potreben zaradi javnega interesa – tudi če tretja država

ne zagotovi ustrezne ravni varstva. Po navedbah predložitvenega sodišča v zadevi C-698/15 lahko ministrstvo za notranje zadeve izda potrdilo nacionalne varnosti, s katerim nekatere podatke izvzame iz spoštovanja določb, ki jih določa zakonodaja.

43 V točki 8.1 tega kodeksa je opozorjeno, da je RIPA uvedel Interception of Communications Commissioner (pooblaščenec za prestrezanje komunikacij, Združeno kraljestvo), čigar naloga je opravljanje neodvisnega nadzora nad izvrševanjem in izvajanjem pooblastil in nalog iz poglavja II dela I zakona RIPA. Točka 8.3 tega kodeksa določa, da ta pooblaščenec lahko, če „ugotovi, da je kakršna koli namerna ali malomarna napaka škodljivo vplivala na posameznika“, to osebo obvesti o domnevni nezakoniti uporabi pooblastil.

Spora o glavni stvari in vprašanja za predhodno odločanje

Zadeva C-203/15

44 Družba Tele2 Sverige (ponudnik elektronskih komunikacijskih storitev s sedežem na Švedskem) je 9. aprila 2014 PTS obvestila, da bo zaradi razglasitve ničnosti Direktive 2006/24 s sodbo z dne 8. aprila 2014, Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238, v nadaljevanju: sodba Digital Rights) s 14. aprilom 2014 prenehala hraniti podatke v zvezi z elektronskimi komunikacijami, na katere se nanaša LEK, in da bo izbrisala podatke, ki jih je hranila do tega dne.

45 Rikspolisstyrelsen (generalna policijska uprava, Švedska) je 15. aprila 2014 pri PTS vložila pritožbo, ker ji je družba Tele2 Sverige prenehala pošiljati zadevne podatke.

46 Justitieminister (minister za pravosodje, Švedska) je 29. aprila 2014 imenoval posebnega poročevalca za preučitev zadevne švedske ureditve glede na sodbo Digital Rights. Posebni poročevalec je v poročilu z dne 13. junija 2014, naslovljenim „Datalagring, EU-rätt och svensk rätt, št. Ds 2014:23“ (hramba podatkov, pravo Unije in švedsko pravo, v nadaljevanju: poročilo iz leta 2014), ugotovil, da nacionalna zakonodaja v zvezi s hrambo podatkov, kot je določena v členih od 16a do 16f LEK, ni v nasprotju niti s pravom Unije niti z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, podpisano v Rimu 4. novembra 1950 (v nadaljevanju: EKČP). Posebni poročevalec je poudaril, da sodbe Digital Rights ni mogoče razlagati tako, da ne upošteva samega načela splošne in neselektivne hrambe podatkov. Meni, da sodbe Digital Rights tudi ni mogoče razumeti tako, da naj bi Sodišče v njej določilo niz meril, ki morajo biti izpolnjena, da bi zakonodajo lahko šteli za sorazmerno. Pri ugotavljanju skladnosti švedske zakonodaje s pravom Unije bi bilo treba presojati vse okoliščine, kot je obseg hrambe podatkov glede na določbe o dostopu do podatkov, o trajanju njihove hrambe, o njihovem varstvu in njihovi varnosti.

47 Na tej podlagi je PTS 19. junija 2014 obvestila družbo Tele2 Sverige, da s tem, ko ni hranila podatkov, ki jih določa LEK, za obdobje šestih mesecev z namenom boja proti kriminalu, ni izpolnila obveznosti iz nacionalne zakonodaje. Nato je PTS z odredbo z dne 27. junija 2014 družbi Tele2 Sverige odredila, naj najpozneje do 25. julija 2014 zagotovi hrambo teh podatkov.

48 Družba Tele2 Sverige je menila, da je poročilo iz leta 2014 temeljilo na napačni razlagi sodbe Digital Rights in da je bila obveznost hrambe podatkov v nasprotju s temeljnimi pravicami, ki jih zagotavlja Listina, in zato je zoper odredbo z dne 27. junija 2014 vložila tožbo pri Förvaltningsrätten i Stockholm (upravno sodišče v Stockholmu, Švedska). Ker je to sodišče tožbo zavrnilo s sodbo z dne 13. oktobra 2014, je družba Tele2 Sverige zoper to sodbo vložila pritožbo pri predložitvenem sodišču.

49 Predložitveno sodišče meni, da je treba skladnost švedske zakonodaje s pravom Unije presojati glede na člen 15(1) Direktive 2002/58. Čeprav naj bi namreč ta direktiva določila načelo, da je treba podatke o prometu in podatke o lokaciji izbrisati ali predelati v anonimne, takoj ko niso več potrebni za prenos

sporočila, naj bi člen 15(1) uvedel odstopanje od tega načela, ker naj bi državam članicam dovolil, da če je to upravičeno iz razlogov, določenih v tem členu, to obveznost izbrisa podatkov oziroma predelave v anonimne podatke omilijo ali celo določijo hrambo podatkov. Pravo Unije naj bi torej v določenih okoliščinah dopustilo hrambo podatkov v zvezi z elektronskimi komunikacijami.

50 Predložitveno sodišče se vseeno sprašuje, ali je splošna in neselektivna obveznost hrambe podatkov v zvezi z elektronskimi komunikacijami, kakršna je ta v postopku v glavni stvari, ob upoštevanju sodbe Digital Rights združljiva s členom 15(1) Direktive 2002/58 glede na člene 7, 8 in 52(1) Listine. Glede na različna mnenja strank v zvezi s tem bi moralo Sodišče jasno odločiti o tem, ali je, kot to meni družba Tele2 Sverige, splošna in neselektivna hramba podatkov v zvezi z elektronskimi komunikacijami sama po sebi nezdružljiva s členi 7, 8 in 52(1) Listine in ali je treba, kot naj bi izhajalo iz poročila iz leta 2014, združljivost take hrambe podatkov presojati glede na določbe v zvezi z dostopom do podatkov, njihovim varstvom in varnostjo ter trajanjem njihove hrambe.

51 V teh okoliščinah je predložitveno sodišče prekinilo odločanje in Sodišču v predhodno odločanje predložilo ti vprašanji:

„1. Ali je splošna obveznost hrambe podatkov o prometu, ki se nanaša na vse subjekte, vsa sredstva elektronske komunikacije in vse podatke o prometu brez kakršnega koli razlikovanja, omejitev ali izjem za namene boja proti kriminalu […], v skladu s členom 15(1) Direktive 2002/58/ES, če se upoštevajo členi 7, 8 in 52(1) Listine?

2. Če je odgovor na prvo vprašanje nikalen, ali je lahko hramba vendarle dovoljena, kadar:
   (a) je dostop nacionalnih organov do hranjenih podatkov določen, kot je opisano v točkah od 19 do 36 [predložitvene odločbe], in
   (b) so zahteve o zaščiti in varnosti podatkov urejene, kot je opisano v točkah od 38 do 43 [predložitvene odločbe], ter
   (c) je treba vse upoštevne podatke hraniti šest mesecev, računano od dneva konca komunikacije, in jih nato izbrisati, kot je opisano v točki 37 [predložitvene odločbe]?“

Zadeva C-698/15

52 T. Watson, P. Brice in G. Lewis so pri High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (vrhovno sodišče (Anglija in Wales)), oddelek Queens' Bench (upravni senat), Združeno kraljestvo) vsak posebej vložili tožbe zaradi nadzora nad zakonitostjo razdelka 1 DRIPA, v katerih zatrjujejo, da je ta razdelek nezdružljiv s členoma 7 in 8 Listine in s členom 8 EKČP.

53 High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (vrhovno sodišče (Anglija in Wales), oddelek Queens' Bench (upravni senat)) je v sodbi z dne 17. julija 2015 ugotovilo, da sodba Digital Rights določa „obvezne zahteve prava Unije“, ki veljajo za ureditve držav članic glede hrambe podatkov v zvezi s komunikacijami in dostopa do teh podatkov. To sodišče meni, da ker je Sodišče v tej sodbi menilo, da Direktiva 2006/24 ni združljiva z načelom sorazmernosti, tudi nacionalna ureditev z enako vsebino kot ta direktiva ne more biti združljiva s tem načelom. Iz logike utemeljitve sodbe Digital Rights naj bi izhajalo, da zakonodaja, ki določa splošno ureditev hrambe podatkov v zvezi s komunikacijami, krši pravice, ki jih zagotavljata člena 7 in 8 Listine, razen če te zakonodaje ne dopolni ureditev dostopa do podatkov, ki jo določa nacionalno pravo in ki predvidi zadostna jamstva za zaščito teh pravic. Razdelek 1 DRIPA naj torej ne bi bil združljiv s členoma 7 in 8 Listine, ker naj ne bi določal jasnih in natančnih pravil v zvezi z dostopom in uporabo hranjenih podatkov in ker naj za dostop do teh podatkov ne bi določal predhodnega nadzora s strani sodišča ali neodvisnega upravnega organa.

54 Ministrstvo za notranje zadeve je proti tej sodbi vložilo pritožbo pri Court of Appeal (England & Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek), Združeno kraljestvo).

55 To sodišče navaja, da razdelek 1(1) DRIPA ministrstvo za notranje zadeve pooblašča, da brez predhodnega dovoljenja sodišča ali neodvisnega upravnega organa sprejme splošen sistem, ki javnim telekomunikacijskim operaterjem nalaga, da hranijo vse podatke v zvezi z vsemi poštnimi ali telekomunikacijskimi storitvami največ dvanajst mesecev, če oceni, da je ta zahteva nujna in sorazmerna za uresničevanje ciljev, določenih v ureditvi Združenega kraljestva. Tudi če ti podatki ne vključujejo vsebine komunikacije, bi lahko zelo posegli v zasebno življenje uporabnikov komunikacijskih storitev.

56 Predložitveno sodišče v predložitveni odločbi in v sodbi z dne 20. novembra 2015, ki je bila izdana v pritožbenem postopku in s katero je odločilo, da ta predlog za predhodno odločanje predloži Sodišču, navaja, da nacionalna pravila v zvezi s hrambo podatkov nujno spadajo v člen 15(1) Direktive 2002/58 in je treba torej spoštovati zahteve, ki izhajajo iz Listine. Zakonodajalec Unije pa naj v skladu s členom 1(3) te direktive ne bi uskladil pravil v zvezi z dostopom do hranjenih podatkov.

57 Glede učinkov sodbe Digital Rights na vprašanji, ki izvirata iz spora o glavni stvari, predložitveno sodišče navaja, da je v zadevi, v kateri je bila izdana ta sodba, Sodišče odločalo o veljavnosti Direktive 2006/24 in ne o veljavnosti nacionalne ureditve. Zlasti glede na tesno razmerje, ki obstaja med hrambo podatkov in dostopom do teh podatkov, bi bilo neizbežno, da ta direktiva določa več jamstev in da so se v sodbi Digital Rights pri presoji zakonitosti ureditve hrambe podatkov, ki jo določa ta direktiva, analizirala pravila o dostopu do teh podatkov. Sodišče naj torej v tej sodbi ne bi določilo nujnih zahtev, ki se uporabijo v nacionalnih zakonodajah v zvezi z dostopom do podatkov, ki ne izvajajo prava Unije. Poleg tega naj bi bil preudarek Sodišča tesno povezan s ciljem te direktive. Vendar bi bilo treba nacionalno zakonodajo presojati glede na njene cilje in njen kontekst.

58 Glede nujnosti, da se Sodišču predloži predlog za sprejetje predhodne odločbe, predložitveno sodišče izpostavlja dejstvo, da se je do dne sprejetja predložitvene odločbe šest sodišč drugih držav članic, med njimi pet sodišč na zadnji stopnji, pri razglasitvi ničnosti nacionalne zakonodaje sklicevalo na sodbo Digital Rights. Odgovor na zastavljeni vprašanji naj torej ne bi bil očiten in naj bi bil nujen za odločitev o zadevah, o katerih to sodišče odloča.

59 V teh okoliščinah je Court of Appeal (England and Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek)) prekinilo odločanje in Sodišču v predhodno odločanje predložilo ti vprašanji:

„1. Ali sodba Digital Rights (zlasti s točkami od 60 do 62) določa obvezne zahteve prava EU, ki veljajo za nacionalno ureditev države članice glede dostopa do podatkov, hranjenih v skladu z nacionalno zakonodajo, da bi bila skladna s členoma 7 in 8 Listine?

2. Ali sodba Digital Rights širi področje uporabe členov 7 in/ali 8 Listine prek področja uporabe člena 8 EKČP, kot je uveljavljeno v sodni praksi Evropskega sodišča za človekove pravice?“

Postopek pred Sodiščem

60 Predsednik Sodišča je s sklepom z dne 1. februarja 2016, Davis in drugi (C-698/15, neobjavljen, EU:C:2016:70), ugodil predlogu Court of Appeal (England & Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek)), da se zadeva C-698/15 obravnava po hitrem postopku, določenem v členu 105(1) Poslovnika Sodišča.

61 Predsednik Sodišča je s sklepom z dne 10. marca 2016 zadevi C-203/15 in C-698/15 združil za ustni postopek in izdajo sodbe.

Vprašanja za predhodno odločanje

Prvo vprašanje v zadevi C-203/15

62 Kammarrätten i Stockholm (pritožbeno upravno sodišče v Stockholmu) s prvim vprašanjem v zadevi C-203/15 v bistvu sprašuje, ali je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, kakršna je ta v postopku v glavni stvari, ki z namenom boja proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov v zvezi z vsemi sredstvi elektronskih komunikacij.

63 To vprašanje izvira med drugim iz dejstva, da je bila Direktiva 2006/24, katere prenos je bil cilj nacionalne ureditve iz postopka v glavni stvari, razglašena za nično s sodbo Digital Rights, vendar mnenje strank ni enotno glede obsega te sodbe in njenih učinkov na to ureditev, ki ureja hrambo podatkov o prometu in podatkov o lokaciji ter dostop nacionalnih organov do teh podatkov.

64 Najprej je treba preučiti, ali nacionalna ureditev, kakršna je ta v postopku v glavni stvari, spada na področje uporabe prava Unije.

Področje uporabe Direktive 2002/58

65 Države članice, ki so predložile pisna stališča Sodišču, so izrazile različna mnenja glede tega, ali in koliko nacionalne ureditve v zvezi s hrambo podatkov o prometu in podatkov o lokaciji in o dostopu nacionalnih organov do teh podatkov s ciljem boja proti kriminalu spadajo na področje uporabe Direktive 2002/58. Medtem ko so belgijska, danska, nemška in estonska vlada, Irska in nizozemska vlada izrazile mnenje, da je treba na to vprašanje odgovoriti pritrdilno, je češka vlada predlagala nikalni odgovor in navedla, da je edini namen teh ureditev boj proti kriminalu. Vlada Združenega Kraljestva je navedla, da na področje uporabe te direktive spadajo le ureditve v zvezi s hrambo podatkov, ne pa ureditve o dostopu nacionalnih organov kazenskega pregona do teh podatkov.

66 Nazadnje, čeprav je Komisija v pisnih stališčih, ki jih je predložila Sodišču v zadevi C-203/15, navedla, da nacionalna ureditev iz postopka v glavni stvari spada na področje uporabe Direktive 2002/58, je v pisnih stališčih v zadevi C-698/15 navedla, da na področje uporabe te direktive spadajo le nacionalna pravila o hrambi podatkov, ne pa nacionalna pravila o dostopu nacionalnih organov do teh podatkov. Zadnja bi bilo po njenem mnenju treba upoštevati pri presoji, ali nacionalna ureditev, ki ureja hrambo podatkov s strani ponudnikov elektronskih komunikacijskih storitev, pomeni sorazmerni poseg v temeljne pravice, ki jih zagotavljata člena 7 in 8 Listine.

67 V zvezi s tem je treba navesti, da je treba pri presoji obsega področja uporabe Direktive 2002/58 upoštevati predvsem njeno splošno sistematiko.

68 Člen 1(1) Direktive 2002/58 med drugim določa uskladitev nacionalnih določb, ki so potrebne za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obravnavo osebnih podatkov na področju elektronskih komunikacij.

69 Člen 1(3) te direktive s področja uporabe te direktive izključuje „dejavnosti države“ na področjih, ki so v njem navedena, in sicer med drugim za dejavnosti države na področju kazenskega prava in dejavnosti v zvezi z javno varnostjo, obrambo, državno varnostjo, vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo (glej po analogiji v zvezi s členom 3(2), prva alinea, Direktive 95/46 sodbi z dne 6. novembra 2003, Lindquist, C-101/01, EU:C:2003:596, točka 43, in z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia, C-73/07, EU:C:2008:727, točka 41).

70 Člen 3 Direktive 2002/58 določa, da se ta direktiva uporabi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave (v nadaljevanju: elektronske komunikacijske storitve). Zato je treba šteti, da ta direktiva ureja dejavnosti ponudnikov teh storitev.

71 Člen 15(1) Direktive 2002/58 določa, da lahko države članice, ob upoštevanju pogojev, ki jih določa, sprejmejo „zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive“. Člen 15(1), drugi stavek, te direktive primeroma opredeljuje ukrepe, ki jih države članice lahko tako sprejmejo, in sicer ukrepe, „ki določajo zadrževanje podatkov“.

72 Zakonski ukrepi iz člena 15(1) Direktive 2002/58 se sicer nanašajo na dejavnosti držav ali drugih državnih organov, ki niso povezane s področji dejavnosti posameznikov (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 51). Poleg tega se nameni, ki jim morajo v skladu s to določbo slediti ti ukrepi, v tem primeru zaščita državne varnosti, obrambe in javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nepooblaščene uporabe elektronskega komunikacijskega sistema, v bistvenem prekrivajo z nameni, ki jih uresničujejo dejavnosti iz člena 1(3) te direktive.

73 Vendar glede na splošno sistematiko Direktive 2002/58 na podlagi elementov, navedenih v prejšnji točki te sodbe, ni mogoče sklepati, da bi bili zakonski ukrepi iz člena 15(1) Direktive 2002/58 izključeni s področja uporabe te direktive, saj bi bil s tem tej določbi odvzet polni učinek. Ta določba namreč nujno predpostavlja, da nacionalni ukrepi, ki so v njej navedeni, kot so ti v zvezi z zadrževanjem podatkov z namenom boja proti kriminalu, spadajo na področje uporabe te direktive, ker zadnjenavedena državam članicam izrecno dopušča, da jih sprejmejo le ob upoštevanju pogojev, ki jih določa.

74 Poleg tega zakonski ukrepi iz člena 15(1) Direktive 2002/58 za namene, navedene v tej določbi, urejajo dejavnost ponudnikov elektronskih komunikacijskih storitev. Zato je treba člen 15(1) v povezavi s členom 3 te direktive razlagati tako, da ti zakonski ukrepi spadajo na področje uporabe te direktive.

75 Zlasti na to področje uporabe spada zakonski ukrep, kakršen je ta v postopku v glavni stvari, ki tem ponudnikom nalaga, da hranijo podatke o prometu in podatke o lokaciji, saj takšna dejavnost nujno zahteva, da ti ponudniki obdelajo osebne podatke.

76 Na to področje uporabe spada tudi zakonski ukrep, ki se nanaša, kot v postopku v glavni stvari, na dostop nacionalnih organov do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev.

77 Varstvo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu, ki ga zagotavlja člen 5(1) Direktive 2002/58, se uporablja za ukrepe, ki so jih sprejele vse osebe razen uporabnikov, ne glede na to, ali gre za zasebne osebe ali subjekte ali državne organe. Kot potrjuje uvodna izjava 21 te direktive, je njen namen preprečiti nedovoljen „dostop“ do sporočil, vključno „z vsemi podatki glede teh sporočil“, da se zagotovi zaupnost elektronskih sporočil.

78 V teh okoliščinah se zakonski ukrep, s katerim država članica na podlagi člena 15(1) Direktive 2002/58 za namene, navedene v tej določbi, nalaga ponudnikom elektronskih komunikacijskih storitev, da nacionalnim organom pod pogoji, ki jih določa ta ukrep, odobrijo dostop do podatkov, ki jih hranijo ti ponudniki, nanaša na obdelavo osebnih podatkov s strani teh ponudnikov, pri čimer gre za obdelavo, ki spada na področje uporabe te direktive.

79 Ker so poleg tega podatki hranjeni le za to, da se – če je to potrebno – pristojnim nacionalnim organom omogoči dostop do teh podatkov, nacionalna ureditev, ki določa hrambo podatkov, načeloma nujno predpostavlja obstoj določb o dostopu pristojnih nacionalnih organov do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev.

80 To razlago podpira člen 15(1)(b) Direktive 2002/58, v skladu s katerim morajo ponudniki na podlagi nacionalnih določb, sprejetih na podlagi člena 15(1) te direktive, vzpostaviti notranje postopke za odzivanje na zahteve za dostop do osebnih podatkov uporabnikov.

81 Iz zgoraj navedenega izhaja, da nacionalna ureditev, kakršna je ta iz postopkov v glavni stvari v zadevah C-203/15 in C-698/15, spada na področje uporabe Direktive 2002/58.

Razlaga člena 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine

82 Navesti je treba, da v skladu s členom 1(2) Direktive 2002/58 njene določbe „podrobno opredeljujejo in dopolnjujejo“ Direktivo 95/46. Direktiva 2002/58 želi, kot je navedeno v njeni uvodni izjavi 2, zlasti zagotoviti popolno spoštovanje pravic, določenih v členih 7 in 8 Listine. V zvezi s tem iz obrazložitve predloga direktive Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (COM (2000) 385 final), na podlagi katerega je bila sprejeta Direktiva 2002/58, izhaja, da je zakonodajalec Unije želel „še naprej zagotavljati visoko raven varstva osebnih podatkov in zasebnosti za vse elektronske komunikacijske storitve ne glede tehnologijo, ki se uporablja“.

83 Zato Direktiva 2002/58 vsebuje posebne določbe, katerih namen je, kot izhaja med drugim iz njenih uvodnih izjav 6 in 7, zavarovanje uporabnikov elektronskih komunikacijskih storitev pred tveganji za njihove osebne podatke in zasebnost, ki izhajajo iz novih tehnologij in čedalje večje zmogljivosti samodejnega shranjevanja in obdelave.

84 Člen 5(1) te direktive zlasti določa, da države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev.

85 Načelo zaupnosti komunikacij, uvedeno z Direktivo 2002/58, med drugim določa, kot izhaja iz njenega člena 5(1), drugi stavek, prepoved vsem osebam razen uporabnikom, da brez privolitve zadevnih uporabnikov shranjujejo podatke o prometu, povezane z elektronskimi komunikacijami. Izjeme so le osebe, ki jim je v skladu s členom 15(1) te direktive to zakonsko dovoljeno, in tehnično shranjevanje, ki je potrebno za prenos sporočila (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 47).

86 Kot potrjujeta uvodni izjavi 22 in 26 Direktive 2002/58, sta torej obdelava in shranjevanje podatkov o prometu na podlagi člena 6 te direktive dovoljena le v obsegu in trajanju, ki sta potrebna za zaračunavanje, trženje in za zagotovitev storitev z dodano vrednostjo (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točki 47 in 48). Zlasti za zaračunavanje storitev je taka obdelava dovoljena samo do poteka obdobja, v katerem se lahko obračun zakonito izpodbija ali se sprožijo postopki za pridobitev plačila. Ko se to obdobje konča, je treba podatke, ki so bili obdelani in shranjeni, izbrisati ali predelati v anonimne. Glede podatkov o lokaciji, ki niso podatki o prometu, člen 9(1) navedene direktive določa, da se smejo takšni podatki obdelati pod določenimi pogoji in šele potem, ko postanejo anonimni, ali s privolitvijo uporabnikov ali naročnikov.

87 Pomen določb členov 5, 6 in 9(1) Direktive 2002/58, ki zagotavljajo zaupnost komunikacij in z njimi povezanih podatkov in ki minimalizirajo tveganja zlorabe, je prav tako treba presojati glede na uvodno izjavo 30 te direktive, v skladu s katero morajo biti „[s]istemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev […] zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum“.

88 Države članice imajo na podlagi člena 15(1) Direktive 2002/58 možnost, da določijo izjeme od načelne obveznosti, navedene v členu 5(1) te direktive, da zagotavljajo zaupnost osebnih podatkov in s tem povezanih obveznosti, navedenih predvsem v členih 6 in 9 navedene direktive (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 50).

89 Ne glede na to je treba člen 15(1) Direktive 2002/58, ker državam članicam dopušča, da omejijo obseg načelne obveznosti zagotavljanja zaupnosti komunikacij in z njimi povezanih podatkov o prometu, v skladu z ustaljeno sodno prakso Sodišča razlagati ozko (glej po analogiji sodbo z dne 22. novembra 2012, Probst, C-119/12, EU:C:2012:748, točka 23). Taka določba torej ne more upravičiti tega, da odstopanje od te načelne obveznosti in zlasti od prepovedi hrambe teh podatkov, ki je določeno v členu 5 te direktive, postane pravilo, saj bi se sicer tej določbi v veliki meri odvzel pomen.

90 V zvezi s tem je treba navesti, da člen 15(1), prvi stavek, Direktive 2002/58 določa, da mora biti namen zakonskih ukrepov iz tega člena, ki odstopajo od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, „zaščita državne varnosti (to je Državne varnosti), obramba, javna varnost […] in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih [kaznivih] dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema“ ali morajo imeti drug cilj, naveden v členu 13(1) Direktive 95/46, na katerega napotuje člen 15(1), prvi stavek, Direktive 2002/58 (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 53). Tako naštevanje namenov je izčrpno, kot to izhaja iz člena 15(1), drugi stavek, te direktive, v skladu s katerim morajo biti zakonski ukrepi upravičeni iz „razlogov“ iz člena 15(1), prvi stavek, navedene direktive. Zato lahko države članice te ukrepe sprejmejo le zaradi ciljev, navedenih v tej zadnji določbi, in ne zaradi drugih ciljev.

91 Poleg tega člen 15(1), tretji stavek, Direktive 2002/58 določa, da so „[v]si ukrepi iz [člena 15(1) te direktive] […] v skladu s splošnimi načeli zakonodaje [Unije], vključno s tistimi iz člena 6(1) in (2) [EU]“, med katerimi so splošna načela in temeljne pravice, ki jih zdaj zagotavlja Listina. Člen 15(1) Direktive 2002/58 je treba torej razlagati glede na temeljne pravice, ki jih zagotavlja Listina (glej po analogiji v zvezi z Direktivo 95/46 sodbe z dne 20. maja 2003, Österreichischer Rundfunk in drugi, C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 68; z dne 13. maja 2014, Google Spain in Google, C-131/12, EU:C:2014:317, točka 68, in z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 38).

92 V zvezi s tem je treba poudariti, da se zaradi obveznosti ponudnikov elektronskih komunikacijskih storitev, ki jo določa nacionalna ureditev, kakršna je ta v postopku v glavni stvari, da hranijo podatke o prometu, da se, če je to potrebno, pristojnim nacionalnim organom omogoči dostop do teh podatkov, ne pojavita le vprašanji v zvezi s spoštovanjem členov 7 in 8 Listine, ki sta izrecno navedeni v vprašanjih za predhodno odločanje, ampak tudi vprašanje v zvezi s svobodnim izražanjem, določenim v členu 11 Listine (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točki 25 in 70).

93 Pri razlagi člena 15(1) Direktive 2002/58 je treba torej upoštevati pomembnost pravice do zasebnega življenja, ki jo zagotavlja člen 7 Listine, in pravice do varstva osebnih podatkov, ki jo zagotavlja člen 8 te listine, kot izhaja iz sodne prakse Sodišča (glej v tem smislu sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 39 in navedena sodna praksa). Enako velja za pravico do svobodnega izražanja glede na poseben pomen, ki jo ima ta svoboščina v vseh demokratičnih družbah. Ta temeljna pravica, zagotovljena v členu 11 Listine, je eden od glavnih temeljev demokratične in pluralistične družbe, ki je del vrednot, na katerih v skladu s členom 2 PEU temelji Unija (glej v tem smislu sodbi z dne 12. junija 2003, Schmidberger, C-112/00, EU:C:2003:333, točka 79, in z dne 6. septembra 2011, Patriciello, C-163/10, EU:C:2011:543, točka 31).

94 V zvezi s tem je treba opozoriti, da mora biti v skladu s členom 52(1) Listine kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, predpisano z zakonom in da je treba spoštovati bistveno vsebino teh pravic. Ob upoštevanju načela sorazmernosti so omejitve pravic in svoboščin dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih (sodba z dne 15. februarja 2016, N., C-601/15 PPU, EU:C:2016:84, točka 50).

95 Nazadnje, člen 15(1), prvi stavek, Direktive 2002/58 določa, da lahko države članice sprejmejo ukrep, ki odstopa od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, kadar je „potreben, primeren in ustrezen znotraj demokratične družbe“ glede na cilje te določbe. V uvodni izjavi 11 te direktive je pojasnjeno, da mora biti tak ukrep „dosledno“ sorazmeren z namenom. Člen 15(1), drugi stavek, navedene direktive zlasti glede hrambe podatkov zahteva, da se ta ukrep sprejme le „za določeno obdobje“ in če je to „upravičeno“ s cilji, navedenimi v členu 15(1), prvi stavek, iste direktive.

96 Spoštovanje načela sorazmernosti izhaja tudi iz ustaljene sodne prakse Sodišča, v skladu s katero varstvo temeljne pravice do spoštovanja zasebnega življenja na ravni Unije zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno (sodbe z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia, C-73/07, EU:C:2008:727, točka 56; z dne 9. novembra 2010, Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, EU:C:2010:662, točka 77; Digital Rights, točka 52, in z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 92).

97 Glede vprašanja ali nacionalna ureditev, kakršna je ta v postopku v glavni stvari v zadevi C-203/15, izpolnjuje te pogoje, je treba navesti, da določa splošno in neselektivno hrambo vseh podatkov o prometu in podatke o lokaciji za vse naročnike in registrirane uporabnike glede vseh elektronskih komunikacijskih sredstev, in da ponudnikom elektronskih komunikacijskih storitev nalaga, naj brez izjeme te podatke hranijo sistematično in kontinuirano. Kot izhaja iz predložitvene odločbe, kategorije podatkov iz te ureditve v bistvu ustrezajo tistim, za katere je hrambo določala Direktiva 2006/24.

98 Na podlagi podatkov, ki jih morajo torej hraniti ponudniki elektronskih komunikacijskih storitev, je mogoče najti in identificirati vir ter namembni kraj komunikacije, določiti datum, uro in vrsto komunikacije, komunikacijsko opremo uporabnikov ter določiti lokacijo opreme za mobilno komunikacijo. Med temi podatki so med drugim ime in naslov naročnika ali registriranega uporabnika, kličoča in klicana telefonska številka ter IP naslov za internetne storitve. Na podlagi teh podatkov je mogoče predvsem izvedeti, s katero osebo je komuniciral naročnik ali registrirani uporabnik in katero sredstvo je uporabil za to, ter ugotoviti trajanje komunikacije in kraj, s katerega je potekala komunikacija. Poleg tega ti podatki omogočajo ugotoviti pogostost komunikacij naročnika ali registriranega uporabnika z nekaterimi osebami v danem obdobju (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 26).

99 Na podlagi vseh teh podatkov je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi teh oseb in socialna okolja, ki jih obiskujejo (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 27). Zlasti so ti podatki sredstva za ugotavljanje, kot je generalni pravobranilec navedel v točkah 253, 254 in od 257 do 259 sklepnih predlogov, profila zadevnih oseb, kar so zelo občutljive informacije glede pravice do spoštovanja zasebnega življenja ter same vsebine komunikacij.

100 Poseg, ki jo taka ureditev pomeni za temeljni pravici, ki jih zagotavljata člena 7 in 8 Listine, se izkaže za širok in ga je treba obravnavati kot posebno resnega. Okoliščina, da se hramba podatkov izvede, ne da bi bili uporabniki elektronskih komunikacijskih storitev o tem obveščeni, lahko pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 37).

101 Čeprav taka ureditev ne dovoljuje hrambe vsebine komunikacije in zato ne more škodovati bistveni vsebini teh pravic (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 39), bi hramba podatkov o prometu in podatkov o lokaciji vendar lahko vplivala na uporabo elektronskih komunikacijskih sredstev in posledično na to, kako uporabniki teh sredstev uresničujejo svojo pravico do svobodnega izražanja, ki jo zagotavlja člen 11 Listine (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 28).

102 Glede na resnost posega v zadevne temeljne pravice, ki jo pomeni nacionalna ureditev, ki za boj proti kriminalu določa hrambo podatkov o prometu in podatkov o lokaciji, lahko ta ukrep upraviči le boj proti hudemu kriminalu (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 60).

103 Poleg tega, čeprav je učinkovitost boja proti hudemu kriminalu, zlasti organiziranem kriminalu in terorizmu, lahko v veliki meri odvisna od uporabe sodobnih tehnik preiskave, tak cilj splošnega interesa, čeprav temeljen, sam po sebi ne more upravičiti tega, da se nacionalna ureditev, ki določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji, šteje za potrebno za namen tega boja (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 51).

104 V zvezi s tem je treba na eni strani navesti, da je učinek take ureditve glede na njene značilnosti, ki so opisane v točki 97 te sodbe, to, da je hramba podatkov o prometu in podatkov o lokaciji pravilo, ureditev, ki jo je uvedla Direktiva 2002/58, pa zahteva, da je ta hramba podatkov izjema.

105 Na drugi strani nacionalna ureditev, kakršna je ta v postopku v glavni stvari, ki na splošno zajema vse naročnike in registrirane uporabnike in se nanaša na vsa elektronska komunikacijska sredstva in na vse podatke o prometu, ne določa nobenega razlikovanja, omejitve ali izjeme glede na cilj, ki se ga poskuša doseči. Nanaša se na splošno na vse osebe, ki uporabljajo elektronske komunikacijske storitve, s tem da te osebe niso – čeprav posredno – v položaju, ki bi lahko pripeljal do kazenskega pregona. Torej se uporablja tudi za osebe, v zvezi s katerimi ni nobenega indica, na podlagi katerega bi bilo mogoče sklepati, da obstaja povezava, čeprav posredna ali daljna, med njihovimi ravnanji in hudimi kaznivimi dejanji. Poleg tega ne določa nobene izjeme, tako da se uporablja tudi za osebe, katerih komunikacije so v skladu z nacionalnimi predpisi poslovna skrivnost (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točki 57 in 58).

106 Taka ureditev ne zahteva nobene povezave med podatki, za katere se določa hramba, in grožnjo za javno varnost. Predvsem pa ni omejena na hrambo bodisi podatkov v zvezi z začasnim obdobjem in/ali določenim z geografskim območjem in/ali krogom oseb, ki so lahko tako ali drugače vpletene v hudo kaznivo dejanje, bodisi podatkov v zvezi z osebami, ki bi lahko iz drugih razlogov, s tem da bi se hranili njihovi podatki, prispevale k boju proti kriminalu (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 59).

107 Nacionalna ureditev, kakršna je ta v postopku v glavni stvari, torej presega meje nujno potrebnega in je torej ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine.

108 Nasprotno pa člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine ne nasprotuje temu, da država članica sprejme ureditev, ki preventivno dopušča ciljno hrambo podatkov o prometu in podatkov o lokaciji za boj proti hudemu kriminalu, če se hramba podatkov glede kategorij hranjenih podatkov, uporabljenih navedenih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe, omeji le na to, kar je nujno potrebno.

109 Ta nacionalna ureditev mora za to, da ustreza zahtevam, navedenim v prejšnji točki te sodbe, prvič, določiti jasna in natančna pravila, ki urejajo obseg in uporabo takega ukrepa hrambe podatkov in ki določajo minimalne zahteve, tako da imajo osebe, katerih podatki so bili hranjeni, zadostno jamstvo, ki jim omogoča učinkovito varstvo njihovih osebnih podatkov pred tveganji zlorabe. Zlasti mora določiti,

v kakšnih okoliščinah in pod kakšnimi pogoji se lahko preventivno sprejme ukrep hrambe podatkov in s tem zagotovi, da se ta ukrep omeji na nujno potrebno (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 54 in navedena sodna praksa).

110 Drugič, glede vsebinskih pogojev, ki jih mora izpolniti nacionalna ureditev, ki v okviru boja proti kriminalu dopusti preventivno hrambo podatkov o prometu in podatkov o lokaciji, da zagotovi, da se hramba omeji na nujno potrebno, je treba navesti, da čeprav se lahko ti pogoji spreminjajo glede na ukrepe, sprejete z namenom preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, mora hramba podatkov vedno ustrezati objektivnim merilom, ki določajo razmerje med podatki, ki jih je treba hraniti, in uresničevanim ciljem. Zlasti morajo taki pogoji v praksi dejansko omejiti obseg ukrepa in kasneje zadevno javnost.

111 Glede omejitve takega ukrepa glede na potencialno zadevne javnosti in položajev mora nacionalna zakonodaja temeljiti na objektivnih elementih, na podlagi katerih je mogoče opredeliti javnost, katere podatki lahko izkažejo zvezo, vsaj posredno, s hudimi kaznivimi dejanji, da tako ali drugače prispevajo k boju proti hudemu kriminalu ali da preprečijo resno nevarnost za javno varnost. Taka omejitev se lahko zagotovi z geografskim merilom, kadar pristojni nacionalni organi na podlagi objektivnih elementov menijo, da obstaja v enem ali več geografskih območjih visoko tveganje za pripravo ali izvršitev takih dejanj.

112 Glede na vse zgornje ugotovitve je treba na prvo vprašanje v zadevi C-203/15 odgovoriti, da je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki z namenom boja proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev.

Drugo vprašanje v zadevi C-203/15 in prvo vprašanje v zadevi C-698/15

113 Uvodoma je treba navesti, da Kammarrätten i Stockholm (pritožbeno upravno sodišče v Stockholmu) drugo vprašanje v zadevi C-203/15 zastavlja le, če je odgovor na prvo vprašanje v tej zadevi nikalen. To drugo vprašanje pa ni odvisno od splošne ali ciljne hrambe podatkov v smislu, navedenem v točkah od 108 do 111 te sodbe. Zato je treba odgovoriti skupaj na drugo vprašanje v zadevi C-203/15 in na prvo vprašanje v zadevi C-698/15, ki je zastavljeno neodvisno od obsega obveznosti hrambe podatkov, ki naj bi bila naložena ponudnikom elektronskih komunikacijskih storitev.

114 Predložitveni sodišči z drugim vprašanjem v zadevi C-203/15 in prvim vprašanjem v zadevi C-698/15 v bistvu sprašujeta, ali je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji ter zlasti dostopu pristojnih nacionalnih organov do hranjenih podatkov, ne da bi se ta dostop omejil le za namen boja proti hudemu kriminalu, s tem da se ne določi, da mora predhodni nadzor nad tem dostopom opraviti sodišče ali neodvisni upravni organ, in se ne zahteva, da se zadevni podatki hranijo na ozemlju Unije.

115 Glede ciljev, ki lahko upravičijo nacionalno ureditev, ki odstopa od načela zaupnosti elektronskih komunikacij, je treba opozoriti, da je, kot je bilo ugotovljeno v točkah 90 in 102 te sodbe, naštevanje ciljev iz člena 15(1), prvi stavek, Direktive 2002/58 izčrpno, zato mora dostop do hranjenih podatkov dejansko in strogo ustrezati kateremu od teh ciljev. Ker mora biti poleg tega tudi cilj te ureditve povezan z resnostjo posega v temeljne pravice, ki ga povzroči ta dostop, iz tega izhaja, da glede preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj le boj proti hudemu kriminalu lahko upraviči tak dostop do hranjenih podatkov.

116 Glede spoštovanja načela sorazmernosti mora nacionalna ureditev, ki ureja pogoje, v katerih morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do hranjenih podatkov, v skladu s tem, kar je bilo ugotovljeno v točkah 95 in 96 te sodbe, zagotoviti, da je tak dostop mogoč le v mejah tistega, kar je nujno potrebno.

117 Ker morajo biti poleg tega zakonski ukrepi iz člena 15(1) Direktive 2002/58 v skladu z uvodno izjavo 11 te direktive „predmet primernih zaščitnih ukrepov“, mora tak ukrep, kot izhaja iz sodne prakse, navedene v točki 109 te sodbe, določiti jasna in natančna pravila, ki določajo, v katerih okoliščinah in pod kakšnimi pogoji morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do podatkov. Tak ukrep mora biti tudi zakonsko zavezujoč v nacionalnem pravu.

118 Za zagotovitev, da se dostop do hranjenih podatkov pristojnim nacionalnim organom omeji na nujno potrebno, mora seveda nacionalno pravo določiti pogoje, pod katerimi morajo ponudniki elektronskih komunikacijskih storitev zagotoviti ta dostop. Vendar se zadevna nacionalna ureditev ne sme omejiti le na to, da zahteva, da dostop ustreza kateremu od ciljev iz člena 15(1) Direktive 2002/58, čeprav gre za boj proti hudemu kriminalu. Taka nacionalna ureditev mora namreč določiti tudi vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 61).

119 Ker torej ni mogoče šteti, da je splošni dostop do vseh hranjenih podatkov, neodvisno od kakršne koli vezi, tudi posredne, s ciljem, ki se mu sledi, omejen na nujno potrebno, se mora zadevna nacionalna ureditev pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do podatkov naročnikov ali registriranih uporabnikov, opreti na objektivna merila. V zvezi s tem je dostop v povezavi z namenom boja proti kriminalu načeloma mogoče odobriti le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so tako ali drugače povezane s tem kaznivim dejanjem (glej po analogiji sodbo Evropskega sodišča za človekove pravice z dne 4. decembra 2015, Zakharov proti Rusiji, CE:ECHR:2015:1204JUD004714306, točka 260). Vendar bi bilo mogoče v posebnih okoliščinah, kakršne so te, v katerih dejanja terorizma ogrožajo bistvene interese nacionalne varnosti, obrambe ali javne varnosti, dostop do podatkov drugih oseb prav tako odobriti, kadar obstajajo objektivni elementi, na podlagi katerih je mogoče šteti, da bi ti podatki lahko v konkretnem primeru učinkovito prispevali k boju proti takim dejavnostim.

120 Da bi se v praksi zagotovilo popolno spoštovanje teh pogojev, je bistveno, da za dostop pristojnih nacionalnih organov do hranjenih podatkov načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi predhoden nadzor in da se odločba tega sodišča ali tega organa izda na obrazložen predlog, ki se ga predloži v postopku preprečevanja, odkrivanja ali pregona kaznivih dejanj (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točka 62; glej tudi po analogiji v zvezi s členom 8 EKČP sodbo Evropskega sodišča za človekove pravice z dne 12. januarja 2016, Szabó in Vissy proti Madžarski, CE:ECHR:2016:0112JUD003713814, točki 77 in 80).

121 Prav tako je pomembno, da pristojni nacionalni organi, ki jim je bil odobren dostop do hranjenih podatkov, v okviru veljavnih nacionalnih postopkov o tem obvestijo zadevne osebe takoj, ko to sporočilo ne more ogroziti preiskav, ki jih vodijo ti organi. Ta informacija je namreč dejansko nujna, da te osebe lahko uresničijo med drugim pravico do pravnega sredstva, ki je izrecno določena v členu 15(2) Direktive 2002/58 v povezavi s členom 22 Direktive 95/46, če bi bile njihove pravice kršene (glej po analogiji sodbi z dne 7. maja 2009, Rijkeboer, C-553/07, EU:C:2009:293, točka 52, in z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 95).

122 Glede pravil o varnosti in varstvu podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, je treba ugotoviti, da člen 15(1) Direktive 2002/58 državam članicam ne omogoča, da odstopajo od členov 4(1) in 4(1a) te direktive. Ti zadnji določbi zahtevata, da ti ponudniki sprejmejo ustrezne tehnične in organizacijske ukrepe, s katerimi se zagotovi učinkovito varstvo hranjenih

podatkov in prepreči tveganje zlorabe in kakršen koli nepooblaščen dostop do teh podatkov. Glede na količino hranjenih podatkov, občutljivost teh podatkov in tveganje za nezakonit dostop do teh podatkov morajo ponudniki elektronskih komunikacijskih storitev, da zagotovijo celovitost in zaupnost teh podatkov, zagotoviti zelo visoko raven varstva in varnosti z ustreznimi tehničnimi in organizacijskimi ukrepi. Zlasti mora nacionalna ureditev določiti hrambo na ozemlju Unije in nepreklicno uničenje teh podatkov po koncu obdobja njihove hrambe (glej po analogiji v zvezi z Direktivo 2006/24 sodbo Digital Rights, točke od 66 do 68).

123 Države morajo vsekakor zagotoviti, da neodvisni organ zagotovi nadzor nad stopnjo varstva, ki jo zagotavlja pravo Unije glede varstva fizičnih oseb v zvezi z obdelavo osebnih podatkov, saj tak nadzor izrecno zahteva člen 8(3) Listine in v skladu z ustaljeno sodno prakso Sodišča pomeni bistveni element spoštovanja varstva oseb glede obdelave osebnih podatkov. V nasprotnem primeru bi bila osebam, katerih osebni podatki so bili hranjeni, odvzeta pravica – ki jo zagotavlja člen 8(1) in (3) Listine – da pri nacionalnih organih nadzora vložijo zahtevo za varstvo svojih podatkov (glej v tem smislu sodbi Digital Rights, točka 68, in z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točki 41 in 58).

124 Predložitveni sodišči morata preveriti, ali in koliko nacionalni ureditvi v postopkih v glavni stvari spoštujeta zahteve iz člena 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine, kot so pojasnjene v točkah od 115 do 123 te sodbe, glede dostopa pristojnih nacionalnih organov do hranjenih podatkov in glede varstva in ravni varnosti teh podatkov.

125 Glede na vse zgornje ugotovitve je treba na drugo vprašanje v zadevi C-203/15 in na prvo vprašanje v zadevi C-698/15 odgovoriti, da je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni zakonodaji, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji, ter zlasti dostop pristojnih nacionalnih organov do hranjenih podatkov in pri tem v okviru boja proti kriminalu navedenega dostopa ne pogojuje z nameni boja proti hudemu kriminalu, ne da bi določil, da mora nadzor nad navedenim dostopom predhodno opraviti sodišče ali neodvisni upravni organ, in ne da bi zahteval, da se zadevni podatki hranijo na ozemlju Unije.

Drugo vprašanje v zadevi C-698/15

126 Z drugim vprašanjem v zadevi C-698/15 Court of Appeal (England & Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek)) v bistvu sprašuje, ali je Sodišče v sodbi Digital Rights člena 7 in/ali 8 Listine razlagalo širše, kot je Evropsko sodišče za človekove pravice razlagalo člen 8 EKČP.

127 Uvodoma je treba opozoriti, da čeprav so, kot potrjuje člen 6(3) PEU, temeljne pravice, ki jih priznava EKČP, kot splošna načela del prava Unije, ta konvencija, dokler Unija ne postane njena pogodbenica, ni pravni instrument, ki bi bil formalno vključen v pravni red Unije (glej v tem smislu sodbo z dne 15. februarja 2016, N., C-601/15 PPU, EU:C:2016:84, točka 45 in navedena sodna praksa).

128 Razlago Direktive 2002/58, ki je predmet te zadeve, je treba torej podati le glede na temeljne pravice, ki jih zagotavlja Listina (glej v tem smislu sodbo z dne 15. februarja 2016, N., C-601/15 PPU, EU:C:2016:84, točka 46 in navedena sodna praksa).

129 Poleg tega je treba opozoriti, da iz pojasnil k členu 52 Listine izhaja, da je namen njenega člena 52(3) zagotoviti potrebno usklajenost med Listino in EKČP, „ne da bi to škodilo avtonomiji prava Unije in Sodišča Evropske unije“ (sodba z dne 15. februarja 2016, N., C-601/15 PPU, EU:C:2016:84, točka 47). Zlasti, kot izrecno določa člen 52(3), drugi stavek, Listine, člen 52(3), prvi stavek, Listine ne preprečuje tega, da pravo Unije odobri širše varstvo kot EKČP. Temu se ne nazadnje doda dejstvo, da se člen 8 Listine nanaša na drugo temeljno pravico kot člen 7 Listine, ki v EKČP nima enakovredne pravice.

130 Iz ustaljene sodne prakse Sodišča pa izhaja, da namen predloga za sprejetje predhodne odločbe ni oblikovanje posvetovalnih mnenj o splošnih ali hipotetičnih vprašanjih, ampak dejanska potreba po učinkoviti rešitvi spora, ki se nanaša na pravo Unije (glej v tem smislu sodbe z dne 24. aprila 2012, Kamberaj, C-571/10, EU:C:2012:233, točka 41; z dne 26. februarja 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, točka 42, in z dne 27. februarja 2014, Pohotovosť, C-470/12, EU:C:2014:101, točka 29).

131 V tem primeru glede na ugotovitve zlasti iz točk 128 in 129 te sodbe vprašanje, ali varstvo, zagotovljeno členom 7 in 8 Listine, presega varstvo, ki se zagotavlja členu 8 EKČP, ne vpliva na razlago Direktive 2002/58 glede na Listino, ki se obravnava v postopku v glavni stvari v zadevi C-698/15.

132 Tako se ne izkaže, da odgovor na drugo vprašanje v zadevi C-698/15 lahko ponudi elemente razlage prava Unije, ki so potrebni za rešitev tega spora glede na to pravo.

133 Iz tega izhaja, da je drugo vprašanje v zadevi C-698/15 nedopustno.

Stroški

134 Ker je ta postopek za stranke v postopkih v glavni stvari ena od stopenj v postopkih pred predložitvenima sodiščema, ti odločita o stroških. Stroški za predložitev stališč Sodišču, ki niso stroški omenjenih strank, se ne povrnejo.

Iz teh razlogov je Sodišče (veliki senat) razsodilo:

1. **Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, glede na člene 7, 8, 11 in 52(1) Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da nasprotuje nacionalni zakonodaji, ki z namenom boja proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev.**

2. **Člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, glede na člene 7, 8, 11 in 52(1) Listine o temeljnih pravicah je treba razlagati tako, da nasprotuje nacionalni zakonodaji, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji, ter zlasti dostop pristojnih nacionalnih organov do hranjenih podatkov in pri tem v okviru boja proti kriminalu navedenega dostopa ne pogojuje z nameni boja proti hudemu kriminalu, ne da bi določil, da mora nadzor nad navedenim dostopom predhodno opraviti sodišče ali neodvisni upravni organ, in ne da bi zahteval, da se zadevni podatki hranijo na ozemlju Unije.**

3. **Drugo vprašanje, ki ga je postavilo Court of Appeal (England & Wales) (Civil Division) (pritožbeno sodišče (Anglija in Wales) (civilni oddelek), Združeno kraljestvo), ni dopustno.**

Podpisi