



Zbierka súdnych rozhodnutí

ROZSUDOK SÚDNEHO DVORA (veľká komora)

z 21. decembra 2016 *

„Návrh na začatie prejudiciálneho konania — Elektronické komunikácie — Spracovávanie osobných údajov — Dôvernoscť elektronických komunikácií — Ochrana — Smernica 2002/58/ES — Články 5, 6 a 9, ako aj článok 15 ods. 1 — Charta základných práv Európskej únie — Články 7, 8 a 11, ako aj článok 52 ods. 1 — Vnútroštátna právna úprava — Poskytovatelia elektronických komunikačných služieb — Povinnosť všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe — Vnútroštátne orgány — Prístup k údajom — Neexistencia predbežného preskúmania zo strany súdu alebo nezávislého správneho orgánu — Zlučiteľnosť s právom Únie“

V spojených veciach C-203/15 a C-698/15,

ktorých predmetom sú návrhy na začatie prejudiciálneho konania podľa článku 267 ZFEÚ, podané rozhodnutím Kammarrätten i Stockholm (Správny odvolací súd Štokholm, Švédsko) z 29. apríla 2015, doručeným Súdnemu dvoru 4. mája 2015, a rozhodnutím Court of Appeal (England & Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát), Spojené kráľovstvo] z 9. decembra 2015, doručeným Súdnemu dvoru 28. decembra 2015, v konaniach

Tele2 Sverige AB (C-203/15)

proti

Post- och telestyrelsen,

a

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

proti

Tomovi Watsonovi,

Petrovi Briceovi,

Geoffreyemu Lewisovi,

za účasti:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

* Jazyky konania: švédčina a angličtina.

SÚDNY DVOR (veľká komora),

v zložení: predseda K. Lenaerts, podpredseda A. Tizzano, predsedovia komôr R. Silva de Lapuerta, T. von Danwitz (spravodajca), J. L. da Cruz Vilaça, E. Juhász a M. Vilaras, sudcovia A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadžiev, S. Rodin, F. Biltgen a C. Lycourgos,

generálny advokát: H. Saugmandsgaard Øe,

tajomník: C. Strömholm, referentka,

so zreteľom na rozhodnutie predsedu Súdneho dvora z 1. februára 2016, že vec C-698/15 sa prejedná v skrátenom konaní upravenom v článku 105 ods. 1 Rokovacieho poriadku Súdneho dvora,

so zreteľom na písomnú časť konania a po pojednávaní z 12. apríla 2016,

so zreteľom na pripomienky, ktoré predložili:

- Tele2 Sverige AB, v zastúpení: M. Johansson, N. Torgerzon, advokater, a E. Lagerlöf a S. Backman,
- T. Watson, v zastúpení: J. Welch a E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, a D. Rose, QC,
- P. Brice a G. Lewis, v zastúpení: A. Suterwalla a R. de Mello, barristers, R. Drabble, QC, a S. Luke, solicitor,
- Open Rights Group a Privacy International, v zastúpení: D. Carey, solicitor, R. Mehta a J. Simor, barristers,
- The Law Society of England and Wales, v zastúpení: T. Hickman, barrister, a N. Turner,
- švédská vláda, v zastúpení: A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren a L. Swedenborg, splnomocnení zástupcovia,
- vláda Spojeného kráľovstva, v zastúpení: S. Brandon, a L. Christie a V. Kaye, splnomocnení zástupcovia, za právnej pomoci D. Beard, G. Facenna a J. Eadie, QC, S. Ford, barrister,
- belgická vláda, v zastúpení: J.-C. Halleux, S. Vanrie a C. Pochet, splnomocnení zástupcovia,
- česká vláda, v zastúpení: M. Smolek a J. Vlášil, splnomocnení zástupcovia,
- dánska vláda, v zastúpení: C. Thorning a M. Wolff, splnomocnení zástupcovia,
- nemecká vláda, v zastúpení: T. Henze, M. Hellmann a J. Kemper, splnomocnení zástupcovia, za právnej pomoci M. Kottmann a U. Karpenstein, Rechtsanwälte,
- estónska vláda, v zastúpení: K. Kraavi-Käerdi, splnomocnená zástupkyňa,
- Írsko, v zastúpení: E. Creedon, L. Williams a A. Joyce, splnomocnení zástupcovia, za právnej pomoci D. Fennelly, BL,
- španielska vláda, v zastúpení: A. Rubio González, splnomocnený zástupca,
- francúzska vláda, v zastúpení: G. de Bergues, D. Colas, F.-X. Bréchet a C. David, splnomocnení zástupcovia,

- cyperská vláda, v zastúpení: K. Kleanthous, splnomocnená zástupkyňa,
- maďarská vláda, v zastúpení: M. Fehér a G. Koós, splnomocnení zástupcovia,
- holandská vláda, v zastúpení: M. Bulterman, M. Gijzen a J. Langer, splnomocnení zástupcovia,
- poľská vláda, v zastúpení: B. Majczyna, splnomocnený zástupca,
- fínska vláda, v zastúpení: J. Heliskoski, splnomocnený zástupca,
- Európska komisia, v zastúpení: H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira a J. Vondung, splnomocnení zástupcovia,

po vypočutí návrhov generálneho advokáta na pojednávaní 19. júla 2016,

vyhlásil tento

Rozsudok

- 1 Návrhy na začatie prejudiciálneho konania sa týkajú výkladu článku 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, s. 37; Mim. vyd. 13/029, s. 514), zmenenej a doplnenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (Ú. v. EÚ L 337, s. 11, ďalej len „smernica 2002/58“), v spojení s článkami 7 a 8, ako aj článkom 52 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“).
- 2 Tieto návrhy boli predložené v rámci dvoch sporov, a to po prvé v spore medzi Tele2 Sverige AB a Post- och telestyrelsen (švédsky orgán pre dohľad nad poštami a telekomunikáciami, ďalej len „PTS“) vo veci rozhodnutia PTS o uložení príkazu na uchovávanie údajov o prenose dát a údajov o polohe účastníkov a registrovaných užívateľov spoločnosti Tele2 Sverige (vec C-203/15), a po druhé v spore medzi Tomom Watsonom, Petrom Briceom a Geoffreym Lewisom, na strane jednej, a Secretary of State for the Home Department (minister vnútra, Spojené kráľovstvo Veľkej Británie a Severného Írska), na strane druhej, vo veci zlučiteľnosti článku 1 Data Retention and Investigator Powers Act 2014 (zákon o uchovávaní údajov a vyšetrovacích právomociach z roku 2014, ďalej len „DRIPA“) s právom Únie (vec C-698/15).

Právny rámec

Právo Únie

Smernica 2002/58

- 3 Odôvodnenia 2, 6, 7, 11, 21, 22, 26 a 30 smernice 2002/58 stanovujú:

„(2) Táto smernica sa snaží rešpektovať základné práva a dodržiavať princípy uznané najmä [Chartou]. Táto smernica sa snaží najmä o plné zabezpečenie práv stanovených v článkoch 7 a 8 [tejto Charty].

...

- (6) Internet revolucionizoval tradičné trhové štruktúry tým, že poskytuje spoločnú, globálnu infraštruktúru pre ponuku širokého rozsahu elektronických komunikačných služieb. Verejne dostupné elektronické komunikačné služby na internete otvárajú nové možnosti pre užívateľov, no prinášajú aj nové riziká pre ich osobné údaje a súkromie.
- (7) V prípade verejných komunikačných sietí by sa mali stanoviť špecifické právne, regulačné a technické opatrenia, aby boli chránené základné práva a slobody fyzických osôb a legitímne záujmy právnických osôb, najmä z hľadiska zvyšovania kapacity automatického uchovávaní a spracovávaní údajov týkajúcich sa účastníkov a užívateľov.

...

- (11) Podobne ako smernica [Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, s. 31; Mim. vyd. 13/015, s. 355)], sa táto smernica netýka otázok ochrany základných práv a slobôd vzťahujúcich sa k činnostiam, ktoré nie sú upravené právom spoločenstva. Preto nemeňte existujúcu rovnováhu medzi právami jednotlivca na súkromie a možnosťami členských štátov prijať opatrenia uvedené v článku 15 ods. 1 tejto smernice, ktoré sú potrebné na ochranu verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a presadzovanie trestného práva. Následne táto smernica nemá vplyv na možnosť členských štátov zachytávať elektronické správy alebo prijímať iné opatrenia, ak je to nevyhnutné z akýchkoľvek iných dôvodov a v súlade s Európskym dohovorom na ochranu ľudských práv a základných slobôd, interpretovaným rozsudkami súdneho dvora týkajúcimi sa ľudských práv; také opatrenia musia byť primerané, prísne proporcionálne vo vzťahu k zamýšľanému účelu a potrebné v rámci demokratickej spoločnosti a mali by byť predmetom primeranej ochrany v súlade s Európskym dohovorom na ochranu ľudských práv a základných slobôd.

...

- (21) Mali by sa prijať opatrenia na zabránenie neoprávneného prístupu k správam, vrátane prístupu k obsahu a k akýmkoľvek údajom takých správ pomocou verejných komunikačných sietí a verejne dostupných elektronických komunikačných služieb. Vnútroštátne právne predpisy v niektorých členských štátoch len zakazujú úmyselný neoprávnený prístup k správam.
- (22) Zákaz ukladania správ a príslušných prevádzkových dát osobami inými, než sú užívatelia alebo účastníci bez ich súhlasu, nie je určený na zákaz akéhokoľvek automatického, dočasného a prechodného uloženia týchto informácií, pokiaľ sa to uskutočňuje výhradne na účely výkonu prenosu v elektronickej komunikačnej sieti a za predpokladu, že informácie sa neukladajú na dobu dlhšiu, než je nevyhnutné na prenos a riadenie chodu prenosu a že počas doby uloženia je zaručená dôvernosc informácií. ...

...

- (26) Údaje vzťahujúce sa k účastníkom, ktoré sú spracovávané v elektronickej komunikačnej sieti a slúžia na zabezpečenie spojenia a prenos informácií, obsahujú údaje o súkromnom živote fyzických osôb a týkajú sa práva na rešpektovanie ich korešpondencie alebo sa týkajú legitímnych záujmov právnických osôb; také údaje sa môžu ukladať len v rozsahu, aký je potrebný na zabezpečenie služby na účely fakturácie a poplatkov za spojenie a len na limitovanú dobu; akékoľvek ďalšie spracovávanie takých údajov... sa môže povoliť len vtedy, keď účastník s týmto súhlasí na základe úplných a presných informácií poskytovateľa verejne dostupných elektronických komunikačných služieb o druhu ďalšieho spracovania, ktoré zamýšľa vykonať a o právach účastníka nedať alebo odvolať svoj súhlas na také spracovanie...

...

(30) Systémy poskytovania elektronických komunikačných sietí a služieb by mali byť konštruované tak, aby bol obmedzený počet nevyhnutných osobných údajov na minimum. ...“

4 Článok 1 smernice 2002/58, nazvaný „Rozsah platnosti a cieľ“, stanovuje:

„1. Touto smernicou sa ustanovuje harmonizácia vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernosť, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronických komunikačných zariadení a služieb v Spoločenstve.

2. Ustanovenia tejto smernice spodrobňujú a dopĺňajú smernicu [95/46] na účely uvedené v odseku 1. Okrem toho poskytujú ochranu legitímnych záujmov účastníkov, ktorí sú právnickými osobami.

3. Táto smernica sa nevzťahuje na činnosti, ktoré sú mimo pôsobnosti zmluvy o založení Európskych spoločenstiev, ako sú činnosti podľa hlavy V a VI Zmluvy o Európskej únii a v žiadnom prípade na činnosti týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a činnosti v oblasti trestného práva.“

5 Článok 2 smernice 2002/58 s názvom „Definície“ stanovuje:

„Pokiaľ nie je stanovené inak, platia definície v smernici [95/46] a v smernici Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) [Ú. v. ES L 108, 2002, s. 33; Mim. vyd. 13/029, s. 349].

Platia aj tieto definície:

...

b) „prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]“ znamenajú akékoľvek údaje spracovávané na účely prenosu správy v elektronickej komunikačnej sieti alebo na účely fakturácie prenosu;

c) „lokalizačné dáta [údaje o polohe – *neoficiálny preklad*]“ znamenajú akékoľvek údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, udávajúce geografickú polohu koncového zariadenia užívateľa verejne dostupnej elektronickej komunikačnej služby;

d) „správa“ znamená akékoľvek informácie vymieňané alebo prenášané medzi konečným počtom účastníkov pomocou verejne dostupnej elektronickej komunikačnej služby. Toto nezahŕňa akékoľvek informácie prenášané ako časť rozhlasových služieb pre verejnosť v elektronickej komunikačnej sieti, pokiaľ sa informácie nemôžu spájať s identifikovateľným účastníkom alebo užívateľom prijímajúcim informácie;

...“

6 Článok 3 smernice 2002/58, nazvaný „Dotknuté služby“, stanovuje:

„Táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Spoločenstve vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu.“

7 Článok 4 tejto smernice, nazvaný „Bezpečnosť spracovania“, znie takto:

„1. Poskytovateľ verejne dostupnej elektronickej komunikačnej služby musí uskutočniť vhodné technické a organizačné opatrenia na zaručenie bezpečnosti svojej služby, ak je to z hľadiska bezpečnosti siete nevyhnutné aj v spojení s poskytovateľom verejnej komunikačnej siete. So zreteľom na stav techniky a náklady na ich implementáciu, tieto opatrenia musia zaručiť úroveň bezpečnosti primeranú existujúcemu riziku.

1a. Bez toho, aby bola dotknutá smernica [95/46], opatrenia uvedené v odseku 1 zahŕňajú prinajmenšom:

- zabezpečenie prístupu k osobným údajom iba oprávneným zamestnancom na zákonom povolené účely,
- ochranu uložených alebo prenášaných osobných údajov pred náhodným alebo nezákonným zničením, náhodnou stratou alebo zmenou, neoprávneným alebo nezákonným ukladáním, spracovaním, prístupom alebo vyzradením a
- zabezpečenie vykonávania bezpečnostnej politiky vo vzťahu k spracovaniu osobných údajov.

...“

8 Podľa článku 5 smernice 2002/58 nazvaného „Dôvernosť správy“:

„1. Členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ a príslušných prevádzkových dát [údajov o prenose dát – *neoficiálny preklad*] prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronickej komunikačných sietí. Zakážu najmä počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami [údajmi o prenose dát – *neoficiálny preklad*] zo strany iných osôb než sú užívatelia bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1 Tento odsek nebráni technickému uloženiu, ak je to potrebné s cieľom prenosu správy, bez vplyvu na princíp dôvernosti.

...

3. Členské štáty zabezpečia, aby sa ukladanie informácií alebo získavanie prístupu k informáciám, ktoré už boli uložené, v koncovom zariadení účastníka alebo užívateľa povolilo len pod podmienkou, že dotknutý účastník alebo užívateľ dal na to vopred súhlas na základe jasných a komplexných informácií v súlade so smernicou [95/46], okrem iného aj o účeloch spracovania. To nebráni nijakému technickému uloženiu ani prístupu výhradne na účely výkonu prenosu správy prostredníctvom elektronickej komunikačnej siete alebo ak je to nevyhnutne potrebné na to, aby poskytovateľ služieb informačnej spoločnosti, ktoré si účastník alebo užívateľ výslovne vyžiadal, mohol tieto služby poskytnúť.“

9 Článok 6 smernice 2002/58, s názvom „Prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]“, stanovuje:

„1. Prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] týkajúce sa účastníkov a užívateľov, spracovávané a uložené poskytovateľom verejnej komunikačnej siete alebo verejne dostupnej elektronickej komunikačnej služby, sa musia vymazať alebo zanonymniť, ak už naďalej nie sú potrebné na účely prenosu správy, bez vplyvu na odseky 2, 3 a 5 tohto článku a článku 15 ods. 1

2. Prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] potrebné na účely fakturácie účastníka a platby za spojenie sa môžu spracovávať. Také spracovanie je povolené len do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu.

3. Na účely marketingu elektronických komunikačných služieb alebo na poskytovanie služieb s pridanou hodnotou poskytovateľ verejne dostupnej elektronickej komunikačnej služby môže spracúvať údaje uvedené v odseku 1 v rozsahu a počas trvania potrebného na také služby alebo marketing, ak účastník alebo užívateľ, ktorého sa údaje týkajú, dá na to predtým svoj súhlas. Užívatelia alebo účastníci musia mať možnosť kedykoľvek odvolať svoj súhlas na spracovanie údajov.

...

5. Spracovávanie prevádzkových dát [údajov o prenose dát – *neoficiálny preklad*], v súlade s odsekmi 1, 2, 3 a 4, sa musí obmedziť na osoby konajúce na pokyn poskytovateľa verejných komunikačných sietí a verejne dostupných elektronických komunikačných služieb, ktoré sú zodpovedné za fakturovanie alebo riadenie prevádzky, vybavovanie dotazov zákazníkov, odhaľovanie podvodov, marketing elektronických komunikačných služieb alebo poskytovanie služby s pridanou hodnotou, a musí sa obmedziť na to, čo je nevyhnutné na účely takých činností.“

- 10 Článok 9 tejto smernice s názvom „Miestne dáta [údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]“ vo svojom odseku 1 stanovuje:

„Ak sa môžu spracovávať miestne dáta [údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré sa týkajú užívateľov alebo účastníkov verejnej komunikačnej siete alebo verejne dostupných elektronických komunikačných služieb, také údaje sa môžu spracovávať, len keď sú anonymné alebo len so súhlasom užívateľov alebo účastníkov v rozsahu a trvaní nevyhnutnom na poskytovanie služby s pridanou hodnotou. Poskytovateľ služby musí informovať užívateľov alebo účastníkov predtým, než získa ich súhlas o druhu miestnych dát iných, než sú prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré bude spracovávať, o účele a dobe trvania spracovávania a o tom, či budú dáta prenášané tretej strane na účely poskytovania služby s pridanou hodnotou. ...“

- 11 Článok 15 uvedenej smernice, nazvaný „Uplatňovanie niektorých ustanovení smernice [95/46]“, stanovuje:

„1. „Členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie elektronického komunikačného systému podľa článku 13 ods. 1 smernice [95/46]. Na tento účel členské štáty môžu, medzi iným, prijať legislatívne opatrenia umožňujúce zadržanie [uchovávanie – *neoficiálny preklad*] údajov na limitované obdobie, oprávnené z dôvodov stanovených v tomto odseku. Všetky opatrenia uvedené v tomto odseku musia byť v súlade so všeobecnými princípmi práva spoločenstva vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 Zmluvy o Európskej únii.

...

1b. Poskytovatelia stanovujú vnútorné postupy na poskytovanie odpovedí na žiadosti o prístup k osobným údajom užívateľov na základe vnútroštátnych ustanovení prijatých podľa odseku 1. Príslušnému vnútroštátnemu orgánu poskytnú na požiadanie informácie o týchto postupoch, počte prijatých žiadostí, právnych odôvodneniach, na ktoré sa žiadosti odvolávajú, a o odpovediach poskytovateľa.

2. Ustanovenia kapitoly III smernice [95/46] o právnych opravných prostriedkoch, záväznosti a sankciách platia vo vzťahu k ustanoveniam prijatým podľa tejto smernice a vo vzťahu k právam jednotlivcov vyplývajúcim z tejto smernice.

...“

Smernica 95/46

- 12 Článok 22 smernice 95/46, nachádzajúci sa v kapitole III tejto smernice, znie:

„Bez toho, aby bol[i] dotknuté akékoľvek administratívne prostriedky nápravy, pre ktoré sa môže urobiť predpis [ktoré možno podať – *neoficiálny preklad*], okrem iného pred dozorným orgánom uvedeným v článku 28, pred žiadosťou o súhlas súdneho orgánu [pred predložením veci súdnemu orgánu – *neoficiálny preklad*], zabezpečia členské štáty právo každej osoby na súdny opravný prostriedok za akékoľvek porušenie práv, ktoré mu zaručuje vnútroštátne právo, použiteľné na uvedené spracovanie.“

Smernica 2006/24/ES

- 13 Článok 1 smernice Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES (Ú. v. EÚ L 105, 2006, s. 54), s názvom „Predmet úpravy a rozsah pôsobnosti“ v odseku 2 stanovuje:

„Táto smernica sa vzťahuje na prevádzkové údaje [údaje o prenose dát – *neoficiálny preklad*] a údaje o polohe právnických a fyzických osôb a na súvisiace údaje, ktoré sú potrebné na identifikáciu účastníka alebo registrovaného užívateľa. Nevzťahuje sa na obsah elektronických komunikácií a informácie vyžiadané pri použití elektronickej komunikačnej siete.“

- 14 Článok 3 tejto smernice, nazvaný „Povinnosť uchovávať údaje“, stanovuje:

„1. Členské štáty odchylné od článkov 5, 6 a 9 smernice [2002/58] prijímú opatrenia, aby zabezpečili, že údaje uvedené v článku 5 tejto smernice sa uchovávajú v súlade s jej ustanoveniami, v rozsahu v akom sú vytvárané alebo spracúvané poskytovateľmi verejne dostupných elektronických komunikačných služieb alebo verejnej komunikačnej siete v ich pôsobnosti v rámci procesu poskytovania príslušných komunikačných služieb.

2. Povinnosť uchovávať údaje stanovená v odseku 1 zahŕňa uchovávanie údajov uvedených v článku 5 v súvislosti s neúspešnými pokusmi o volanie, ktoré poskytovatelia verejne dostupných elektronických komunikačných služieb alebo verejnej komunikačnej siete vytvárajú alebo spracovávajú a uchovávajú (ak ide o telefónne údaje) alebo ukladajú (ak ide o internetové údaje), v pôsobnosti dotknutého členského štátu a poskytovania týchto komunikačných služieb. Táto smernica nepožaduje uchovávanie údajov, ktoré sa týkajú nespojených volaní.“

Švédske právo

- 15 Z rozhodnutia vnútroštátneho súdu vo veci C-203/15 vyplýva, že švédsky zákonodarca na účely prebratia smernice 2006/24 do vnútroštátneho práva zmenil lagen (2003:389) om elektronisk kommunikation [zákon (2003:389) o elektronických komunikáciách, ďalej len „LEK“] a förordningen (2003:396) om elektronisk kommunikation [vyhláška (2003:396) o elektronických komunikáciách]. Oba

tieto texty, v znení uplatniteľnom na spor vo veci samej, obsahujú pravidlá týkajúce sa uchovávania údajov súvisiacich s elektronickou komunikáciou, ako aj prístupu k týmto údajom zo strany vnútroštátnych orgánov.

- 16 Prístup k týmto údajom upravuje okrem toho lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpande myndigheternas underrättelseverksamhet [zákon (2012:278) o poskytovaní údajov týkajúcich sa elektronických komunikácií pri vyšetrovacích činnostiach orgánov pôsobiacich v oblasti presadzovania práva, ďalej len „zákon 2012:278“), ako aj rättegångsbalken (súdny poriadok, ďalej len „RB“).

O povinnosti uchovávania údajov o elektronických komunikáciách

- 17 Podľa informácií poskytnutých vnútroštátnym súdom vo veci C-203/15 stanovujú ustanovenia kapitoly 6 § 16a LEK v spojení s § 1 kapitoly 2 tohto zákona povinnosť poskytovateľov elektronických komunikačných služieb uchovávať údaje, ktorých povinnosť uchovávania vznikla na základe smernice 2006/24. Ide o údaje týkajúce sa predplatného a všetkých elektronických komunikácií nevyhnutných na vysledovanie a identifikáciu zdroja a adresáta komunikácie, dátumu, času a trvania komunikácie, typu komunikácie, použitého komunikačného zariadenia a polohy použitého mobilného komunikačného zariadenia pri začatí a ukončení komunikácie. Povinnosť uchovávať údaje sa vzťahuje na údaje vytvorené alebo spracované telefónnym spojením, mobilným telefónnym spojením, prenosom správ, internetovým prístupom, ako aj poskytovaním kapacity na internetový prístup (spôsob pripojenia). Táto povinnosť zahŕňa aj údaje týkajúce sa neúspešných komunikácií. Nevzťahuje sa však na obsah týchto komunikácií.
- 18 § 38 až § 43 vyhlášky (2003:396) o elektronických komunikáciách spresňujú kategórie údajov, ktoré sa musia uchovávať. Pokiaľ ide o telefonické služby, musia sa uchovávať údaje o volaniach a o volaných číslach, ako aj o dátumoch a časoch, ktoré sú vysledovateľné od začiatku do skončenia komunikácie. Pokiaľ ide o telefonické služby využívajúce mobilné pripojenie, ukladajú sa dodatočné povinnosti, akými sú napríklad uchovávanie údajov o polohe pri začatí a skončení komunikácie. Pokiaľ ide o telefonické služby využívajúce pakety IP, musia sa najmä uchovávať, okrem údajov uvedených vyššie, aj údaje o IP adresách volajúceho a volaného. Pokiaľ ide o systémy elektronickej pošty, musia sa uchovávať najmä údaje o číslach odosielateľov a príjemcov, IP adresách alebo akákoľvek ďalšia e-mailová adresa. Pokiaľ ide o služby prístupu k internetu, musia sa napríklad uchovávať údaje o IP adresách užívateľov, ako aj o dátumoch a časoch pripojenia k službe prístupu k internetu a odpojenia od nej.

O dobe uchovávania údajov

- 19 V súlade s kapitolou 6 § 16d LEK sa musia údaje uvedené § 16a tejto kapitoly uchovávať poskytovateľmi elektronických komunikačných služieb šesť mesiacov odo dňa ukončenia komunikácie. Potom sa musia údaje okamžite zničiť, pokiaľ sa v § 16d druhom odseku LEK nestanovuje inak.

O prístupe k uchovávaným údajom

- 20 Prístup k údajom uchovávaným vnútroštátnymi orgánmi sa riadi ustanoveniami zákona 2012:278, LEK a RB.

– Zákon 2012:278

- 21 Na základe ustanovení § 1 zákona 2012:278 môžu Säkerhetspolisen (bezpečnostná služba, Švédsko) a Tullverket (colný úrad, Švédsko) v rámci spravodajskej činnosti štátnej polície zbierať za podmienok stanovených týmto zákonom a bez vedomia poskytovateľa elektronickej komunikačnej siete alebo

poskytovateľa elektronických komunikačných služieb oprávneného na základe LEK údaje o správach zaslaných prostredníctvom elektronickej komunikačnej siete, o elektronických komunikačných zariadeniach nachádzajúcich sa v danej zemepisnej oblasti, ako aj v zemepisnej oblasti či oblastiach, v ktorých sa nachádza alebo sa nachádzalo elektronické komunikačné zariadenie.

- 22 Podľa § 2 a § 3 zákona 2012:278 možno údaje v podstate zbierať vtedy, keď má toto opatrenie v závislosti od okolností osobitný význam z hľadiska predchádzania, zabránenia alebo odhaľovania trestnej činnosti zahŕňajúcej jeden alebo viaceré trestné činy, za ktoré možno uložiť trest odňatia slobody aspoň na dva roky, alebo niektorý z trestných činov vymenovaných v § 3 tohto zákona, vrátane priestupkov, za ktoré možno uložiť trest odňatia slobody v dĺžke kratšej ako dva roky. Dôvody na uplatnenie tohto opatrenia musia prevážiť nad úvahami týkajúcimi sa ohrozenia alebo ujmy, ktoré alebo ktorú toto opatrenie spôsobí s ohľadom na toho, proti komu smeruje, alebo s ohľadom na protichodný záujem. V súlade s § 5 uvedeného zákona dĺžka platnosti opatrenia nesmie prekročiť jeden mesiac.
- 23 Rozhodnutie vykonať takéto opatrenie prijíma vedúci príslušného orgánu alebo osoba, ktorá má príslušné poverenie. Toto rozhodnutie nepodlieha predbežnému preskúmaniu zo strany súdneho orgánu alebo nezávislého správneho orgánu.
- 24 Podľa § 6 zákona 2012:278 treba oznámiť Säkerhets- och integritetsskyddsmynden (Komisia pre bezpečnosť a ochranu integrity, Švédsko) každé rozhodnutie o povolení na zhromažďovanie údajov. Podľa § 1 lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [zákon (2007:980) o dohlade nad určitými činnosťami v oblasti presadzovania práva] má tento orgán dohliadať na uplatňovanie práva orgánmi pôsobiacimi v oblasti presadzovania práva.

– LEK

- 25 Podľa ustanovení § 22 prvého odseku bodu 2 kapitoly 6 LEK musí každý poskytovateľ elektronických komunikačných služieb na požiadanie poskytnúť údaje o predplatnom prokurátorovi, polícii, bezpečnostnej službe alebo akémukoľvek inému orgánu verejnej moci poverenému presadzovaním práva, ak tieto údaje súvisia s podozrením zo spáchania trestného činu. Podľa informácií, ktoré poskytol vnútroštátny súd vo veci C-203/15 nie je nevyhnutné, aby išlo o závažný trestný čin.

– RB

- 26 RB upravuje oznamovanie uchovávaných údajov vnútroštátnym orgánom počas vyšetrovaní. V súlade s § 19 kapitoly 27 RB „sledovanie elektronickej komunikácie“ bez vedomia tretej osoby je v zásade prípustné v rámci vyšetrovania týkajúceho sa najmä trestných činov, za ktoré možno uložiť trest odňatia slobody v dĺžke minimálne šesť mesiacov. „Sledovanie elektronických komunikácií“ treba v súlade s § 19 kapitoly 27 RB chápať ako zber údajov bez vedomia tretích osôb o správach zaslaných prostredníctvom elektronickej komunikačnej siete, o elektronických komunikačných zariadeniach, ktoré sa nachádzajú alebo sa nachádzali v určitej zemepisnej oblasti, ako aj zemepisnej oblasti či oblastiach, v ktorých sa nachádza alebo sa nachádzalo elektronické komunikačné zariadenie.
- 27 Podľa informácií poskytnutých vnútroštátnym súdom vo veci C-203/15 nemožno na základe § 19 kapitoly 27 RB zbierať informácie o obsahu správy. Sledovanie elektronických komunikácií možno v zásade nariadiť na základe § 20 kapitoly 27 RB len vtedy, keď existuje dôvodné podozrenie, že určitá osoba spáchala trestný čin a že opatrenie má pre vyšetrovanie osobitný význam, pričom toto vyšetrovanie sa musí okrem toho týkať trestného činu, za ktorý možno uložiť trest odňatia slobody v dĺžke aspoň dvoch rokov, alebo pokusu, prípravy alebo účasti v zločineckej skupine na účely spáchania takého trestného činu. V súlade s ustanovením § 21 kapitoly 27 RB musí prokurátor – okrem naliehavých prípadov – skôr, než pristúpi k sledovaniu elektronickej komunikácie, požiadať príslušný súd o povolenie.

O bezpečnosti a ochrane uchovávaných údajov

- 28 Podľa ustanovenia § 3 kapitoly 6 a LEK majú poskytovatelia elektronických komunikačných služieb, ktorí sú povinní uchovávať údaje, prijať vhodné technické a organizačné opatrenia nevyhnutné na zabezpečenie ochrany údajov počas ich spracovania. Podľa informácií poskytnutých vnútroštátnym súdom vo veci C-203/15 však švédske právo neupravuje ustanovenia o mieste uchovávania údajov.

Právo Spojeného kráľovstva

DRIPA

- 29 Článok 1 DRIPA, nazvaný „Právomoc uchovávať údaje o relevantných komunikáciách podliehajúcich ochrane“, stanovuje:

„(1) [Minister vnútra] môže príkazom (ďalej len „príkaz na uchovávanie údajov“) nariadiť verejnému telekomunikačnému operátorovi, aby uchovával relevantné údaje týkajúce sa komunikácií, ak dospeje k záveru, že táto požiadavka je nevyhnutná a primeraná vo vzťahu k jednému alebo viacerým účelom, ktoré spadajú pod článok 22 ods. 2 písm. a) až h) Regulation of Investigatory Powers Act 2000 [zákon o úprave vyšetrovacích právomocí z roku 2000] (účely, na ktoré možno získať údaje o prenose dát).

(2) Príkaz na uchovávanie údajov môže:

- a) sa vzťahovať na konkrétneho poskytovateľa alebo určitú kategóriu poskytovateľov;
- b) vyžadovať uchovávanie všetkých údajov alebo určitej kategórie údajov;
- c) uvádzať jedno alebo viaceré obdobia, počas ktorých sa majú údaje uchovávať;
- d) obsahovať iné požiadavky alebo obmedzenia v súvislosti s uchovávaním údajov;
- e) zavádzať odlišné ustanovenia na rôzne účely;
- f) súvisieť s údajmi, ktoré existujú alebo neexistujú v čase vydania alebo nadobudnutia právoplatnosti príkazu.

(3) [Minister vnútra] môže vyhláškou prijať podrobnejšie ustanovenia týkajúce sa uchovávania relevantných údajov o prenose dát.

(4) Taká úprava sa môže týkať najmä:

- a) požiadaviek pred vydaním príkazu na uchovávanie údajov;
- b) maximálnej doby, počas ktorej sa majú údaje podľa príkazu na uchovávanie údajov uchovávať;
- c) obsahu, vydania, nadobudnutia právoplatnosti, preskúmania, zmeny alebo zrušenia príkazu na uchovávanie údajov;
- d) celistvosti, zabezpečenia alebo ochrany uchovávaných údajov na základe tohto článku, prístupu k nim alebo ich zverejnenia či zničenia;
- e) vymáhania alebo kontroly dodržiavania relevantných požiadaviek alebo obmedzení;

- f) kódexu osvedčených postupov súvisiaceho s relevantnými požiadavkami alebo obmedzeniami alebo relevantnými právomocami;
- g) (podmienečnej alebo bezpodmienečnej) náhrady výdavkov vynaložených verejnými telekomunikačnými operátormi pri plnení relevantných požiadaviek alebo obmedzení zo strany [ministra vnútra];
- h) skončenia účinnosti [Data Retention (EC Directive) Regulations 2009 (vyhláška o uchovávaní údajov v zmysle smernice ES z roku 2009)] a prechodu k uchovávaniu údajov na základe tohto článku.

(5) Maximálna doba stanovená na základe odseku 4 písm. b) nesmie byť dlhšia ako 12 mesiacov a počíta sa odo dňa stanoveného v súvislosti s predmetnými údajmi vyhláškou podľa odseku 3.

...“

- 30 Článok 2 DRIPA vymedzuje pojem „relevantné údaje o prenose dát“ ako „také údaje o prenose dát, aké sú uvedené v prílohe vyhlášky o uchovávaní údajov v zmysle smernice ES z roku 2009, pokiaľ také údaje vytvoria alebo spracujú v Spojenom kráľovstve verejní telekomunikační operátori v procese poskytovania predmetných telekomunikačných služieb“.

RIPA

- 31 Článok 21 zákona o úprave vyšetrovacích právomocí z roku 2000 (ďalej len „RIPA“), ktorý sa nachádza v kapitole II tohto zákona s názvom „Získanie a sprístupňovanie údajov o prenose dát“, vo svojom odseku 4 spresňuje:

„V tejto kapitole sa pod pojmom ‚údaje o prenose dát‘ rozumejú:

- a) akékoľvek údaje o prenose dát zahrnuté v komunikácii alebo pripojené k nej (buď odosielateľom, alebo inak) na účely akejkoľvek poštovej služby alebo telekomunikačného systému, prostredníctvom ktorých sa tieto údaje prenášajú alebo môžu prenášať;
- b) akékoľvek informácie, ktoré nezahŕňajú žiadny obsah komunikácie [okrem akýchkoľvek informácií, ktoré spadajú pod písmeno a)] a z ktorých vyplýva, že ktokoľvek používa:
 - i) akúkoľvek poštovú službu alebo telekomunikačnú službu alebo
 - ii) akúkoľvek časť telekomunikačného systému v súvislosti s tým, že ktokoľvek poskytuje alebo používa akúkoľvek telekomunikačnú službu,
- c) akékoľvek informácie, ktoré nespádajú pod písmeno a) alebo b) a ktoré uchováva alebo získa osoba poskytujúca poštovú službu alebo telekomunikačnú službu v súvislosti s osobami, ktorým poskytuje túto službu.“

- 32 Podľa informácií uvedených v návrhu na začatie prejudiciálneho konania vo veci C-698/15 tieto údaje zahŕňajú „údaje o polohe užívateľa“, ale nespĺňajú požiadavky týkajúce sa obsahu oznámenia.

- 33 Pokiaľ ide o prístup k uchovávaným údajom, článok 22 smernice RIPA stanovuje:

„(1) Tento článok sa uplatní, pokiaľ zodpovedná osoba na účely tejto kapitoly považuje za nevyhnutné z dôvodov podľa odseku 2 tohto článku získať akékoľvek údaje o prenose dát.“

(2) Z dôvodov podľa tohto odseku je nevyhnutné získať údaje o prenose dát, ak sú potrebné:

- a) v záujme národnej bezpečnosti;
- b) na účely predchádzania alebo odhaľovania trestnej činnosti alebo narušenia verejného poriadku;
- c) v záujme hospodárskej prosperity Spojeného kráľovstva;
- d) v záujme verejnej bezpečnosti;
- e) na ochranu verejného zdravia;
- f) na vyrubenie alebo výber akejkoľvek dane, cla, odvodu alebo iného poplatku, príspevku alebo dávky, ktoré sa platia štátnemu orgánu;
- g) ak ide o naliehavú situáciu, na predchádzanie úmrtiam, zraneniam alebo akémukoľvek poškodeniu telesného alebo duševného zdravia ľudí alebo na zmiernenie akéhokoľvek zranenia alebo poškodenia telesného alebo duševného zdravia ľudí;
- h) na akýkoľvek iný účel [(nespadajúci pod písmená a) až g)] uvedený v príkaze, ktorý vydá [minister vnútra].

(4) S výhradou podľa odseku 5 môže zodpovedná osoba, ak sa domnieva, že telekomunikačný operátor alebo prevádzkovateľ poštových služieb má k dispozícii údaje, alebo by mohol mať tieto údaje k dispozícii, požiadať návrhom od telekomunikačného alebo poštového operátora, aby tento operátor

- a) získal údaje, pokiaľ ich nemá ešte k dispozícii, a
- b) poskytol v každom prípade všetky informácie, ktoré má k dispozícii, alebo ktoré neskôr získa.

(5) Zodpovedná osoba nesmie udeliť povolenie podľa odseku 3 alebo predložiť žiadosť podľa odseku 4, ak dospeje k záveru, že získanie predmetných informácií vyplývajúcich z povoleného alebo vyžadovaného konania na základe povolenia alebo žiadosti je primerané k cieľu, na aký sa majú tieto údaje získať.“

- 34 V súlade s článkom 65 RIPA, ak má niekto dôvod domnievať sa, že údaje boli získané protiprávne, možno sťažnosti predkladať Investigatory Powers Tribunal (súd pre kontrolu vyšetrovacích právomocí, Spojené kráľovstvo).

Data Retention Regulations 2014

- 35 Data Retention Regulations 2014 (vyhláška z roku 2014 o uchovávaní údajov), prijatá na základe DRIPA, sa delí na tri časti, pričom druhá z nich zahŕňa články 2 až 14 tejto vyhlášky. Článok 4 nazvaný „Žiadosti v oblasti uchovávania“ stanovuje:

„(1) Žiadosti v oblasti uchovávania musia presne uvádzať:

- a) verejného telekomunikačného operátora (alebo opis operátorov), ktorým je určená;
- b) príslušné údaje o prenose dát, ktoré sa majú uchovávať;
- c) jedno alebo viaceré obdobia, počas ktorých sa majú údaje uchovávať;

d) akúkoľvek inú požiadavku alebo obmedzenie v súvislosti s uchovávaním údajov.

(2) V žiadosti o uchovávanie nemožno vyžadovať, aby sa údaje uchovávali dlhšie ako 12 mesiacov:

- a) v prípade údajov o prenose dát a údajov o využívaní služieb, odo dňa predmetného oznámenia a
- b) v prípade údajov o účastníkoch, odo dňa, keď dotknutá osoba ukončí predmetné komunikačné služby, alebo odo dňa, keď dôjde k zmene údajov (ak táto nastane skôr).

...“

36 Podľa článku 7 tejto vyhlášky, nazvaného „Celistvosť a bezpečnosť údajov“:

„(1) Verejný telekomunikačný operátor, ktorý uchováva údaje podľa článku 1 [DRIPA] musí:

- a) sa ubezpečiť, že údaje majú rovnakú celistvosť a podliehajú rovnakému stupňu zabezpečenia a ochrany ako údaje zo systémov, z ktorých pochádzajú;
- b) zabezpečiť prostredníctvom primeraných technických a organizačných opatrení, aby len osobitne poverení zamestnanci mohli mať prístup k údajom, a
- c) chrániť údaje primeranými technickými a organizačnými opatreniami proti nezákonnému zničeniu, strate alebo náhodnému pozmeneniu, alebo pred nezákonným či nepovoleným uchovávaním, spracovávaním, prístupom alebo zverejnením.

(2) Verejný telekomunikačný operátor, ktorý uchováva údaje o prenose dát podľa článku 1 [DRIPA], musí zničiť údaje, ak ich uchovávanie už nie je povolené podľa tohto článku, a nie je inak povolené podľa zákona.

(3) Požiadavka uvedená v odseku 2 zničiť údaje predstavuje požiadavku vymazať údaje tak, aby prístup k nim nebol možný.

(4) Z pohľadu operátora stačí prijať opatrenia, aby k mazaniu údajov dochádzalo mesačne alebo v kratších intervaloch podľa možností prevádzkovateľa v praxi.“

37 Článok 8 uvedenej vyhlášky, nazvaný „Sprístupnenie uchovávaných údajov“, stanovuje:

„(1) Verejný telekomunikačný operátor musí zaviesť primerané bezpečnostné systémy (vrátane technických a organizačných opatrení), ktorými sa určuje prístup k údajom o prenose dát uchovávaným podľa článku 1 [DRIPA] s cieľom zabrániť akémukoľvek zverejneniu, ktoré nespadá pod článok 1 ods. 6 písm. a) [DRIPA].

(2) Verejný telekomunikačný operátor, ktorý uchováva údaje podľa článku 1 [DRIPA], musí uchovávať údaje tak, aby sa dali na základe žiadosti sprístupniť bez zbytočného odkladu.“

38 Článok 9 tej istej vyhlášky, nazvaný „Preskúmanie komisárom pre ochranu osobných údajov“, stanovuje:

„Komisár pre ochranu osobných údajov musí preskúmať dodržanie požiadaviek alebo obmedzení uvedených v tejto časti súvisiacich s celistvosťou, bezpečnosťou a zničením údajov uchovávaných podľa článku 1 [DRIPA].“

Kódex postupov

- 39 Akquisition and disclosure of Communications Data Code of Practice (kódex osvedčených postupov na získanie a sprístupňovanie údajov o prenose dát, ďalej len „kódex postupov“) stanovuje vo svojich odsekoch 2.5 až 2.9 a 2.36 až 2.45 usmernenia o nevyhnutnosti a primeranosti získavanie údajov o prenose dát. Podľa vysvetlení vnútroštátneho súdu vo veci C-698/15 treba osobitnú pozornosť v súlade s odsekmi 3.72 až 3.77 tohto kódexu venovať nevyhnutnosti a primeranosti v prípade, keď sa požadované údaje o prenose dát týkajú osoby vykonávajúcej povolanie, v ktorom sa zaoberá s údajmi chránenými služobným tajomstvom alebo ktoré sú inak dôverné.
- 40 Podľa odsekov 3.78 až 3.84 uvedeného kódexu sa súdny príkaz vyžaduje v osobitnom prípade žiadosti o prístup k údajom o prenose dát podanej na účely identifikácie novinárskeho zdroja. V súlade s odsekmi 3.85 až 3.87 tohto istého kódexu sa súdne povolenie vyžaduje v prípade žiadosti o prístup podanej miestnymi orgánmi. Na sprístupnenie údajov o prenose dát podliehajúcich podľa zákona profesijnému tajomstvu alebo údajov o prenose dát týkajúcich sa lekárov, poslancov parlamentu alebo duchovných sa nevyžaduje povolenie súdu alebo rozhodnutie pochádzajúce od iného nezávislého orgánu.
- 41 Odsek 7.1 kódexu osvedčených postupov stanovuje, že údaje o prenose dát získané alebo nadobudnuté podľa ustanovení RIPA, ako aj všetky výpisy a zhrnutia a kópie týchto údajov sa musia spracovávať a uchovávať bezpečným spôsobom. Okrem toho požiadavky stanovené v Data Protection Act (zákon o ochrane údajov) musia byť splnené.
- 42 V súlade s odsekom 7.18 kódexu osvedčených postupov, pokiaľ orgán verejnej moci Spojeného kráľovstva zvažuje možnosť sprístupniť údaje o prenose dát cudzím štátnym orgánom, musí najmä preskúmať, či tieto údaje budú vhodne chránené. Z odseku 7.22 tohto kódexu však vyplýva, že prenos údajov do tretích krajín sa môže uskutočniť, ak je tento prevod potrebný z dôvodov dôležitého verejného záujmu, a to aj vtedy, ak tretia krajina nezabezpečuje vhodnú úroveň ochrany. Podľa informácií od vnútroštátneho súdu vo veci C-698/15 môže minister vnútra v tejto súvislosti vydať osvedčenie o národnej bezpečnosti, ktoré oslobodzuje určité údaje od povinnosti spĺňať ustanovenia upravené v právnych predpisoch.
- 43 V odseku 8.1 uvedeného kódexu sa pripomína, že RIPA zriaďuje funkciu Interception of Communications Commissioner (komisár pre dohľad nad odpočúvaním, Spojené kráľovstvo), ktorého úlohou je najmä nezávisle dohliadať nad výkonom právomocí a povinností stanovených v kapitole II časti I RIPA. Ako vyplýva z odseku 8.3 toho istého kódexu, pokiaľ možno „preukázať, že úmyselným alebo nedbanlivostným konaním došlo k porušeniu práv jednotlivca“, tento komisár je oprávnený, aby oznámil tomuto jednotlivcovi, že vzniklo podozrenie o nezákonnom zneužití právomoci.

Spory vo veciach samých a prejudiciálne otázky

Vec C-203/15

- 44 Dňa 9. apríla 2014 spoločnosť Tele2 Sverige, poskytovateľ elektronických komunikácií so sídlom vo Švédsku, oznámila PTS, že v nadväznosti na zrušenie smernice 2006/24 rozsudkom z 8. apríla 2014, Digital Rights Ireland a i. (C-293/12 a C-594/12, ďalej len „rozsudok Digital Rights“, EU:C:2014:238), prestane od 14. apríla 2014 uchovávať údaje o elektronických komunikáciách uvedené v LEK, a vymaže údaje, ktoré dovtedy uchovávala.
- 45 Dňa 15. apríla 2014 Rikspolisstyrelsen (prezídium policajného zboru, Švédsko) podalo PTS sťažnosť z dôvodu, že Tele2 Sverige prestala jeho útvaram poskytovať predmetné údaje.

- 46 Dňa 29. apríla 2014 justitieminister (minister spravodlivosti, Švédsko) vymenoval osobitného vyšetrovateľa na preskúmanie predmetnej švédskej právnej úpravy v súvislosti s rozsudkom Digital Rights. V správe z 13. júna 2014 nazvanej „Datalagring, EU-rätten och svensk rätt, n° Ds 2014:23“ (uchovávanie údajov, právo Únie a švédske právo, ďalej len „správa z roku 2014“), osobitný vyšetrovateľ dospel k záveru, že vnútroštátna právna úprava o uchovávaní údajov, ako sa uvádza v § 16a až § 16f LEK, nie je v rozpore s právom Únie ani Európskym dohovorom o ochrane ľudských práv a základných slobôd, podpísaným 4. novembra 1950 v Ríme (ďalej len „EDLP“). Osobitný vyšetrovateľ zdôraznil, že rozsudok Digital Rights nemožno vykladať v tom zmysle, že by bránil samotnej zásade všeobecného a nediferencovaného uchovávania údajov. Podľa tohto vyšetrovateľa nemožno rozsudok Digital Rights chápať ani v tom zmysle, že Súdny dvor v ňom stanovil súbor kritérií, ktoré musia byť splnené na to, aby bolo možné považovať právnu úpravu za primeranú. Na overenie súladu švédskej právnej úpravy s právom Únie treba posúdiť všetky okolnosti, akou je rozsah uchovávania údajov vzhľadom na ustanovenia týkajúce sa prístupu k údajom, doby uchovávania údajov, ich ochrany, ako aj ich bezpečnosti.
- 47 Dňa 19. júna 2014 na základe toho PTS Tele2 Sverige oznámil, že si nespĺnila povinnosti stanovené vnútroštátnou právnu úpravou tým, že neuchovávala údaje podľa LEK počas šiestich mesiacov na účely boja proti trestnej činnosti. PTS jej príkazom z 27. júna 2014 následne nariadil, aby najneskôr 25. júla 2014 začala opätovne tieto údaje uchovávať.
- 48 Keďže Tele2 Sverige sa domnievala, že správa z roku 2014 sa zakladala na nesprávnom výklade rozsudku Digital Rights a že povinnosť uchovávať údaje bola v rozpore so základnými právami zaručenými Chartou, podala proti príkazu z 27. júna 2014 žalobu na Förvaltningsrätten i Stockholm (Správny súd Štokholm, Švédsko). Po zamietnutí žaloby týmto súdom rozsudkom z 13. októbra 2014 sa Tele2 Sverige proti tomuto rozsudku odvolala na vnútroštátny súd, ktorý podal návrh na začatie prejudiciálneho konania.
- 49 Podľa vnútroštátneho súdu treba zlučiteľnosť švédskej právnej úpravy s právom Únie posúdiť so zreteľom na článok 15 ods. 1 smernice 2002/58. Hoci sa totiž táto smernica zakladá na zásade, že údaje o prenose dát a polohe sa musia vymazať alebo zanonymniť, ak už naďalej nie sú potrebné na účely prenosu správy, článok 15 ods. 1 tejto smernice zavádza výnimku z tejto zásady, pretože umožňuje členským štátom, ak je to odôvodnené niektorým z dôvodov stanovených v tomto odseku, obmedziť túto povinnosť vymazania alebo anonymizácie či dokonca upraviť povinnosť uchovávania údajov. Podľa práva Únie sa teda umožňuje v určitých situáciách uchovávať údaje o elektronických komunikáciách.
- 50 Vnútroštátny súd sa však pýta, či všeobecná a nediferencovaná povinnosť uchovávať údaje o elektronických komunikáciách, o akú ide vo veci samej, je s prihliadnutím na rozsudok Digital Rights zlučiteľná s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7 a 8, ako aj článkom 52 ods. 1 Charty. Vzhľadom na rozdielne názory účastníkov konania v tejto súvislosti je potrebné, aby Súdny dvor jednoznačne rozhodol o otázke, či – ako tvrdí Tele2 Sverige – všeobecná a nediferencovaná povinnosť uchovávať údaje o elektronických komunikáciách je sama osebe nezlučiteľná s článkami 7 a 8, ako aj s článkom 52 ods. 1 Charty, alebo či – ako vyplýva zo správy z roku 2014 – zlučiteľnosť takéhoto uchovávania sa musí posúdiť vzhľadom na ustanovenia týkajúce sa prístupu k údajom, ich ochrany a bezpečnosti, ako aj doby ich uchovávania.
- 51 Za týchto okolností vnútroštátny súd rozhodol prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:
- „1. Je všeobecná povinnosť uchovávať údaje vzťahujúca sa na všetky osoby, všetky prostriedky elektronickej komunikácie a všetky údaje o prenose dát bez akéhokoľvek rozlišovania, obmedzení alebo výnimiek na účely boja proti trestnej činnosti s prihliadnutím na články 7 a 8 a článok 52 ods. 1 Charty zlučiteľná s článkom 15 ods. 1 smernice 2002/58?

2. V prípade, ak je odpoveď na prvú otázku záporná, možno uchovávanie napriek tomu povoliť, pokiaľ:
- a) prístup vnútroštátnych orgánov k uchovávaným údajom je vymedzený tak, ako je to opísané v bodoch 19 až 36 [návrhu na začatie prejudiciálneho konania] a
 - b) požiadavky na ochranu a bezpečnosť údajov sú upravené tak, ako je to opísané v bodoch 38 až 43 [návrhu na začatie prejudiciálneho konania] a
 - c) všetky relevantné údaje sa majú uchovávať šesť mesiacov odo dňa ukončenia komunikácie a následne sa majú vymazať tak, ako je to opísané v bode 37 [návrhu na začatie prejudiciálneho konania]?”

Vec C-698/15

- 52 Páni Watson, Brice a Lewis jednotlivo podali na High Court of Justice (England and Wales), Queen's Bench Division (Divisional Court) [Vyšší súd (Anglicko a Wales), Queen's Bench Division (správna komora), Spojené kráľovstvo], žaloby o preskúmanie zákonnosti článku 1 DRIPA, pričom sa odvolávali najmä na nezlučiteľnosť tohto článku s článkami 7 a 8 Charty, ako aj s článkom 8 EDLP.
- 53 Rozsudkom zo 17. júla 2015 High Court of Justice (England and Wales), Queen's Bench Division (Divisional Court) [Vyšší súd (Anglicko a Wales), Queen's Bench Division (správna komora), Spojené kráľovstvo], rozhodol, že rozsudok Digital Rights stanovoval „záväzné požiadavky práva Únie“ uplatniteľné na právne úpravy členských štátov v oblasti uchovávania údajov o prenose dát, ako aj na prístup k týmto údajom. Podľa tohto súdu, keďže Súdny dvor v uvedenom rozsudku dospel k záveru, že smernica 2006/24 je nezlučiteľná so zásadou proporcionality, ani vnútroštátna právna úprava, ktorá má rovnaký obsah ako táto smernica, nemôže byť v súlade s touto zásadou. Z logiky, z ktorej vychádza rozsudok Digital Rights, vyplýva, že právna úprava stanovujúca všeobecný režim uchovávania údajov o prenose dát porušuje práva zakotvené v článkoch 7 a 8 Charty, pokiaľ táto právna úprava nie je doplnená režimom prístupu k údajom, ktorý je definovaný vnútroštátnym právom a ktorý poskytuje dostatočné záruky na ochranu týchto práv. Článok 1 DRIPA nie je zlučiteľný s článkami 7 a 8 Charty, pretože nestanovuje jasné a presné pravidlá vzťahujúce sa na prístup a používanie uchovávaných údajov a nepodmieňuje prístup k takýmto údajom predchádzajúcemu preskúmaniu vykonanému súdom alebo nezávislým správnym orgánom.
- 54 Minister vnútra sa proti tomuto rozsudku odvolal na Court of Appeal (England & Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát), Spojené kráľovstvo].
- 55 Tento súd, uvedený ako posledný, uvádza, že článok 1 ods. 1 DRIPA splnomocňuje ministra vnútra, aby bez predchádzajúceho povolenia súdu alebo nezávislého správneho orgánu stanovil všeobecný režim zaväzujúci verejných telekomunikačných operátorov uchovávať všetky údaje o všetkých poštových alebo telekomunikačných službách po dobu najviac 12 mesiacov, za predpokladu, že sa domnieva, že táto požiadavka je potrebná a primeraná vzhľadom na ďalšie účely stanovené v právnej úprave Spojeného kráľovstva. Hoci tieto údaje nezahŕňajú obsah komunikácie, mohli by mať osobitne rušivý charakter, pokiaľ ide o súkromie používateľov komunikačných služieb.
- 56 Vnútroštátny súd sa v návrhu na začatie prejudiciálneho konania a vo svojom rozsudku z 20. novembra 2015 vydanom v rámci odvolacieho konania, v ktorom rozhodol predložiť Súdnu dvoru prejednávaný návrh na začatie prejudiciálneho konania, domnieva, že vnútroštátne pravidlá o uchovávaní údajov spadajú nevyhnutne pod článok 15 ods. 1 smernice 2002/58, a preto musia spĺňať požiadavky vyplývajúce z Charty. Z článku 1 ods. 3 tejto smernice však vyplýva, že normotvorca Únie nevykonala harmonizáciu pravidiel týkajúcich sa prístupu k uchovávaným údajom.
- 57 Pokiaľ ide o vplyv rozsudku Digital Rights na otázky nastolené v spore vo veci samej, vnútroštátny súd uvádza, že vo veci, ktorá viedla k vydaniu daného rozsudku, sa Súdny dvor zaoberal platnosťou smernice 2006/24, a nie platnosťou vnútroštátnej právnej úpravy. Vzhľadom na úzky vzťah existujúci medzi uchovávaním údajov a prístupom k týmto údajom bolo teda podľa vnútroštátneho súdu

potrebné, aby sa k smernici pridal rad záruk a aby sa v rámci rozsudku Digital Rights v rámci preskúmania zákonnosti systému ochrany údajov zavedeného uvedenou smernicou analyzovali pravidlá prístupu k týmto údajom. Súdny dvor teda neplánoval stanoviť v uvedenom rozsudku záväzné požiadavky, ktoré by sa vzťahovali na vnútroštátne právne úpravy týkajúce sa prístupu k údajom, ktorými by sa neuplatňovalo právo Únie. Navyše odôvodnenie Súdneho dvora bolo úzko spojené s cieľom sledovaným práve touto smernicou. Vnútroštátnu právnu úpravu však treba posudzovať vzhľadom na jej ciele, ktoré sleduje, a jej kontext.

- 58 Pokiaľ ide o nevyhnutnosť podať na Súdny dvor návrh na začatie prejudiciálneho konania, vnútroštátny súd zdôrazňuje skutočnosť, že ku dňu prijatia rozhodnutia vnútroštátneho súdu šesť súdov iných členských štátov, z ktorých päť poslednej inštancie, zrušili na základe rozsudku Digital Rights vnútroštátne právne úpravy. Odpoveď na položené otázky nie je teda zrejmá a okrem toho je nevyhnutná na posúdenie vecí, o ktorých tento súd rozhoduje.
- 59 Za týchto okolností Court of Appeal (England and Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát)] rozhodol prerušiť konanie a položil Súdnemu dvoru tieto prejudiciálne otázky:
- „1. Stanovuje rozsudok Digital Rights (a to najmä body 60 až 62 tohto rozsudku) záväzné požiadavky práva Únie uplatniteľné na vnútroštátny režim členského štátu, ktorý upravuje prístup k údajom uchovávaným v súlade s vnútroštátnymi právnymi predpismi, aby boli dodržané články 7 a 8 Charty?
2. Rozširuje rozsudok Digital Rights rozsah pôsobnosti článkov 7 a/alebo 8 Charty nad rámec rozsahu pôsobnosti článku 8 EDLP, ako je stanovená v judikatúre Európskeho súdu pre ľudské práva?“

O konaní pred Súdnym dvorom

- 60 Uznesením z 1. februára 2016, Davis a i. (C-698/15, EU:C:2016:70), predseda Súdneho dvora rozhodol vyhovieť návrhu Court of Appeal (England & Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát)] na prejednanie veci C-698/15 v skrátenom súdnom konaní podľa článku 105 ods. 1 Rokovacieho poriadku Súdneho dvora.
- 61 Rozhodnutím predsedu Súdneho dvora z 10. marca 2016 boli veci C-203/15 a C-698/15 spojené na účely ústnej časti konania a vyhlásenia rozsudku.

O prejudiciálnych otázkach

O prvej otázke vo veci C-203/15

- 62 Svojou prvou otázkou vo veci C-203/15 sa Kamarrätten i Stockholm (Odvolací správny súd Štokholm) v podstate pýta, či sa má článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7 a 8, ako aj s článkom 52 ods. 1 Charty vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, o akú ide vo veci samej, ktorá na účely boja proti trestnej činnosti stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie.
- 63 Táto otázka vychádza najmä z tej skutočnosti, že smernica 2006/24, ktorú vnútroštátna právna úprava vo veci samej má za cieľ prebrať, bola vyhlásená za neplatnú rozsudkom Digital Rights, no účastníci konania majú rozdielny názor, pokiaľ ide o dosah tohto rozsudku a jeho vplyv na uvedenú právnu úpravu týkajúcu sa uchovávania údajov o prenose dát a polohe, ako aj prístupu k týmto údajom vnútroštátnymi orgánmi.

- 64 V prvom rade treba preskúmať, či vnútroštátna právna úprava, o akú ide vo veci samej, spadá do pôsobnosti práva Únie.

Rozsah pôsobnosti smernice 2002/58

- 65 Členské štáty, ktoré Súdnemu dvoru predložili písomné pripomienky, vyslovili rozdielne názory na otázku, či a v akom rozsahu vnútroštátne právne úpravy týkajúce sa uchovávaní údajov o prenose dát a polohe, ako aj prístupu k týmto údajom zo strany vnútroštátnych orgánov na účely boja proti trestnej činnosti, spadajú do pôsobnosti smernice 2002/58. Kým totiž najmä belgická, dánska, nemecká, estónska vláda a Írsko, ako aj holandská vláda vyjadrili názor, že táto otázka si vyžaduje kladnú odpoveď, česká vláda navrhuje, aby Súdny dvor odpovedal na túto otázku záporne, pričom uvádza, že jediným cieľom týchto právnych úprav je boj proti trestnej činnosti. Vláda Spojeného kráľovstva pritom tvrdí, že do pôsobnosti tejto smernice spadajú len právne úpravy o uchovávaní údajov, a nie tie, ktoré sa týkajú prístupu k týmto údajom zo strany príslušných vnútroštátnych orgánov v oblasti boja proti trestnej činnosti.
- 66 Pokiaľ ide napokon o Komisiu, táto vo svojich písomných pripomienkach predložených Súdnemu dvoru vo veci C-203/15 síce tvrdila, že vnútroštátna právna úprava dotknutá vo veci samej spadá do pôsobnosti smernice 2002/58, vo svojich písomných pripomienkach vo veci C-698/15 však uviedla, že do pôsobnosti smernice spadajú len vnútroštátne pravidlá o uchovávaní údajov, no nepatria tam už pravidlá, ktoré sa týkajú prístupu vnútroštátnych orgánov k týmto údajom. Pravidlá o prístupe k údajom by sa však mali podľa nej zohľadniť s cieľom posúdiť, či vnútroštátna právna úprava stanovujúca uchovávanie údajov poskytovateľmi elektronických komunikačných služieb predstavuje primeraný zásah do základných práv zaručených článkami 7 a 8 Charty.
- 67 V tejto súvislosti treba uviesť, že rozsah pôsobnosti smernice 2002/58 treba posúdiť so zreteľom najmä na všeobecnú systematiku tejto smernice.
- 68 Podľa článku 1 ods. 1 smernice 2002/58 táto smernica stanovuje najmä harmonizáciu vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernitosť, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore.
- 69 Podľa článku 1 ods. 3 tejto smernice sa z jej pôsobnosti vylučujú „činnosti štátu“ v oblastiach, ktoré sú v nej uvedené, t. j. najmä činnosti štátu v oblasti trestného práva, ako aj tie, ktoré sa týkajú ochrany verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) (pozri analogicky, pokiaľ ide o článok 3 ods. 2 prvú zarážku smernice 95/46, rozsudky zo 6. novembra 2003, Lindqvist, C-101/01, EU:C:2003:596, bod 43, ako aj zo 16. decembra 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727, bod 41).
- 70 Článok 3 smernice 2002/58 stanovuje, že táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Únii vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu (ďalej len „služby elektronickej komunikácie“). Z toho vyplýva, že uvedenú smernicu treba považovať za upravujúcu činnosti poskytovateľov takých služieb.
- 71 Článok 15 ods. 1 smernice 2002/58 umožňuje členským štátom prijať za podmienok, ktoré stanovuje, „legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice“. Článok 15 ods. 1 druhá veta uvedenej smernice uvádza ako príklady opatrení, ktoré teda môžu prijať členské štáty, opatrenia „umožňujúce uchovávanie údajov“.

- 72 Je isté, že legislatívne opatrenia uvedené v článku 15 ods. 1 smernice 2002/58 predstavujú činnosti štátu alebo štátnych orgánov a nepatria do oblasti činností jednotlivcov (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 51). Okrem toho účely, ktoré musia podľa tohto ustanovenia tieto opatrenia spĺňať – v predmetnom prípade ochrana národnej bezpečnosti, obrana a verejná bezpečnosť, ako aj zabránenie trestným činom, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávneného používania elektronického komunikačného systému – sa výrazne prekrývajú s cieľmi sledovanými činnosťami uvedenými v článku 1 ods. 3 tejto smernice.
- 73 Vzhľadom na všeobecnú systematiku smernice 2002/58 nemožno na základe skutočností uvedených v predchádzajúcom bode tohto rozsudku dospieť k záveru, že legislatívne opatrenia uvedené v článku 15 ods. 1 smernice 2002/58 sú vyňaté z pôsobnosti tejto smernice, pretože inak by bolo toto ustanovenie zbavené všetkého potrebného účinku. Dané ustanovenie totiž nevyhnutne predpokladá, že vnútroštátne opatrenia, ktoré sú v ňom uvedené, ako napríklad opatrenia na uchovávanie údajov na účely boja proti trestnej činnosti, spadajú do rozsahu pôsobnosti tejto smernice, pretože táto smernica výslovne dovoľuje členským štátom prijať také opatrenia len za určitých podmienok, ktoré sú v nej stanovené.
- 74 Okrem toho legislatívne opatrenia, ktoré sú uvedené v článku 15 ods. 1 smernice 2002/58, upravujú na účely uvedené v tomto ustanovení činnosť poskytovateľov elektronických komunikačných služieb. Z tohto dôvodu sa má uvedený článok 15 ods. 1 v spojení s článkom 3 danej smernice vykladať v tom zmysle, že takéto legislatívne opatrenia spadajú do pôsobnosti tejto smernice.
- 75 Do tejto pôsobnosti spadá najmä legislatívne opatrenie, o aké ide vo veci samej, ktoré týmto poskytovateľom ukladá povinnosť uchovávať údaje o prenose dát a polohe, pretože takáto činnosť nevyhnutne znamená spracúvanie osobných údajov týmito poskytovateľmi.
- 76 Do uvedenej pôsobnosti spadá aj legislatívne opatrenie, ktoré sa týka, ako je to vo veci samej, prístupu vnútroštátnych orgánov k údajom uchovávaným poskytovateľmi elektronických komunikačných služieb.
- 77 Ochrana dôvernosti elektronických komunikácií a údajov o prenose dát súvisiacich s elektronickými komunikáciami, ktorá je zaručená v článku 5 ods. 1 smernice 2002/58, sa totiž vzťahuje na opatrenia, ktoré prijali osoby iné než používatelia, či už ide o súkromné fyzické alebo právnické osoby alebo štátne subjekty. Ako potvrdzuje odôvodnenie 21 tejto smernice, jej cieľom je zabrániť „[akémukoľvek]“ neoprávnenému prístupu k obsahu a k „akýmkoľvek údajom takých správ“ s cieľom chrániť dôvernosť elektronických komunikácií.
- 78 Za týchto okolností legislatívne opatrenie, ktorým členský štát ukladá na základe článku 15 ods. 1 smernice 2002/58 poskytovateľom elektronických komunikačných služieb, aby na účely uvedené v tomto ustanovení poskytli vnútroštátnym orgánom za podmienok stanovených v tomto opatrení prístup k údajom uchovávaným týmito poskytovateľmi, sa týka spracovania osobných údajov, pričom ide o spracovania, ktoré patria do rozsahu pôsobnosti tejto smernice.
- 79 Okrem toho, keďže jediným účelom uchovávania údajov je ich prípadné sprístupnenie príslušným vnútroštátnym orgánom, vnútroštátna právna úprava, ktorá stanovuje uchovávanie údajov, v zásade nevyhnutne zahŕňa existenciu ustanovení týkajúcich sa prístupu príslušných vnútroštátnych orgánov k údajom, ktoré uchovávajú poskytovatelia elektronických komunikačných služieb.
- 80 Tento výklad potvrdzuje článok 15 ods. 1b smernice 2002/58, podľa ktorého poskytovatelia stanovia vnútorné postupy na poskytovanie odpovedí na žiadosti o prístup k osobným údajom užívateľov na základe vnútroštátnych ustanovení prijatých podľa odseku 1.

- 81 Z vyššie uvedeného vyplýva, že taká vnútroštátna právna úprava, o akú ide vo veci samej vo veciach C-203/15 a C-698/15, spadá do pôsobnosti smernice 2002/58.

O výklade článku 15 ods. 1 smernice 2002/58 vzhľadom na články 7, 8 a 11, ako aj článok 52 ods. 1 Charty

- 82 Treba zdôrazniť, že v súlade s článkom 1 ods. 2 smernice 2002/58 ustanovenia tejto smernice „spodrobňujú a dopĺňajú“ smernicu 95/46. Ako sa uvádza v odôvodnení 2, smernica 2002/58 sa snaží najmä o plné zabezpečenie práv uvedených v článkoch 7 a 8 Charty. V tejto súvislosti z dôvodovej správy k návrhu smernice Európskeho parlamentu a Rady týkajúcej sa spracovávanía osobných údajov a ochrany súkromia v sektore elektronických komunikácií [COM (2000) 385 v konečnom znení], na základe ktorej bola prijatá smernica 2002/58, vyplýva, že normotvorca Únie chcel „zabezpečiť, aby aj naďalej bola zaručená vysoká úroveň ochrany osobných údajov a súkromia pre všetky elektronické komunikačné služby, bez ohľadu na použité technológie“.
- 83 Na tento účel smernica 2002/58 obsahuje osobitné ustanovenia, ktorými sa sleduje, ako vyplýva najmä z jej odôvodnení 6 a 7, ochrana používateľov elektronických komunikačných služieb pred rizikami pre osobné údaje a súkromie, ktoré vyplývajú z nových technológií a zo zvyšovania kapacity automatického uchovávanía a spracovávanía údajov.
- 84 Článok 5 ods. 1 tejto smernice predovšetkým stanovuje, že členské štáty musia svojimi vnútroštátnymi právnymi úpravami zabezpečiť dôvernú komunikáciu a príslušných údajov o prenose dát prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí.
- 85 Zásada dôvernosti komunikácií podľa smernice 2002/58 zahŕňa okrem iného, ako vyplýva z článku 5 ods. 1 druhej vety tejto smernice, že sa akýmkoľvek iným osobám než používateľom v zásade zakazuje bez súhlasu týchto používateľov uchovávať údaje o prenose dát, týkajúce sa elektronickej komunikácie. Predmetom výnimiek sú len osoby oprávnené zákonom v súlade s článkom 15 ods. 1 tejto smernice a technické uchovávanie, ktoré je nevyhnutné na účely prenosu správy (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 47).
- 86 Ako to teda potvrdzujú odôvodnenia 22 a 26 smernice 2002/58, spracúvanie a uchovávanie údajov o prenose dát je v súlade s článkom 6 tejto smernice povolené len v rozsahu a na obdobie potrebné na účely fakturácie služieb, ich marketingu alebo poskytovania služieb s pridanou hodnotou (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, body 47 a 48). Pokiaľ ide osobitne o fakturáciu služieb, také spracovanie je povolené len do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu. Po uplynutí tejto doby sa údaje, ktoré boli spracúvané a uchovávané, musia vymazať alebo zanonymizovať. Pokiaľ ide o údaje o polohe iné, než sú údaje o prenose dát, článok 9 ods. 1 uvedenej smernice stanovuje, že takéto údaje sa môžu spracovávať len za určitých podmienok, a potom, ako boli anonymizované, alebo so súhlasom užívateľov alebo účastníkov.
- 87 Rozsah pôsobnosti ustanovení článkov 5 a 6 a článku 9 ods. 1 smernice 2002/58, ktoré sa týkajú zabezpečenia dôvernosti komunikácie a súvisiacich údajov, ako aj minimalizovania rizík zneužitia, treba navyše posúdiť s ohľadom na odôvodnenie 30 tejto smernice, podľa ktorého „systémy poskytovania elektronických komunikačných sietí a služieb by mali byť konštruované tak, aby bol obmedzený počet nevyhnutných osobných údajov na minimum“.
- 88 Článok 15 ods. 1 smernice 2002/58 umožňuje členským štátom zaviesť výnimky z povinnosti stanovenej v článku 5 ods. 1 uvedenej smernice, podľa ktorej sú tieto štáty povinné zabezpečiť dôvernú osobných údajov, ako aj z príslušných povinností uvedených najmä v článkoch 6 a 9 uvedenej smernice (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 50).

- 89 Keďže však článok 15 ods. 1 smernice 2002/58 umožňuje členským štátom obmedziť rozsah základnej povinnosti, ktorou je zabezpečiť dôvernosť údajov o prenose dát súvisiacich s elektronickými komunikáciami, v súlade s ustálenou judikatúrou Súdneho dvora ho treba vykladať reštriktívne (pozri analogicky rozsudok z 22. novembra 2012, Probst, C-119/12, EU:C:2012:748, bod 23). Takéto ustanovenie nemôže teda odôvodniť, že výnimka z tejto zásadnej povinnosti, a najmä výnimka zo zákazu uchovávať tieto údaje stanovená v článku 5 tejto smernice, sa stane pravidlom, pretože v takom prípade by došlo k zbaveniu tohto ustanovenia veľkej časti jeho rozsahu pôsobnosti.
- 90 V tejto súvislosti treba uviesť, že článok 15 ods. 1 prvá veta smernice 2002/58 stanovuje, že cieľom legislatívnych opatrení, ktorých sa týka a ktoré predstavujú výnimku zo zásady dôvernosti údajov o prenose dát súvisiacich s elektronickými komunikáciami, musí byť „zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a zabránenie trestným činom, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávneného používania elektronického komunikačného systému“ alebo musia sledovať niektorý z iných cieľov sledovaných článkom 13 ods. 1 smernice 95/46, na ktorý odkazuje článok 15 ods. 1 prvá veta smernice 2002/58 (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 53). Ako vyplýva z článku 15 ods. 1 druhej vety tej istej smernice, takýto zoznam cieľov je taxatívny, pričom podľa neho všetky legislatívne opatrenia musia byť odôvodnené „z dôvodov stanovených“ v článku 15 ods. 1 prvej vete uvedenej smernice. Členské štáty teda nemôžu prijať takéto opatrenia na iné účely než tie, ktoré sú stanovené v tomto ustanovení.
- 91 Okrem toho článok 15 ods. 1 tretia veta smernice 2002/58 stanovuje, že „všetky opatrenia uvedené v [článku 15 ods. 1 tejto smernice] musia byť v súlade so všeobecnými princípmi práva [Únie] vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 Zmluvy o [EÚ]“, medzi ktorými sa nachádzajú všeobecné zásady a základné práva, ktoré sú teraz zaručené Chartou. Článok 15 ods. 1 smernice 2000/58 treba preto vykladať v spojení so základnými právami zaručenými Chartou (pozri analogicky, pokiaľ ide o smernicu 95/46, rozsudky z 20. mája 2003, Österreichischer Rundfunk a i., C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 68; z 13. mája 2014, Google Spain a Google, C-131/12, EU:C:2014:317, bod 68, ako aj zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 38).
- 92 V tejto súvislosti treba zdôrazniť, že povinnosť uložená poskytovateľom elektronických komunikačných služieb takou vnútroštátnou právnou úpravou, ako je tá vo veci samej, podľa ktorej sú povinní uchovávať údaje o prenose dát na účely ich prípadného sprístupnenia príslušným vnútroštátnym orgánom, vyvoláva otázky týkajúce sa súladu nielen s článkami 7 a 8 Charty, ktoré sú výslovne spomenuté v prejudiciálnych otázkach, ale aj so slobodou prejavu zaručenou v článku 11 Charty (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, body 25 a 70).
- 93 Z tohto dôvodu treba pri výklade článku 15 ods. 1 smernice 2002/58 prihliadať tak na význam práva na rešpektovanie súkromného života zaručeného článkom 7 Charty, ako aj na dôležitosť práva na ochranu osobných údajov zaručeného článkom 8 Charty, ako vyplýva z judikatúry Súdneho dvora (pozri v tomto zmysle rozsudok zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 39 a citovanú judikatúru). To isté platí aj s ohľadom na právo na slobodu prejavu vzhľadom na mimoriadny význam tejto slobody v každej demokratickej spoločnosti. Toto základné právo zaručené článkom 11 Charty predstavuje jednu zo základných podstát demokratickej a pluralitnej spoločnosti odrážajúcej hodnoty, na ktorých je Únia v súlade s článkom 2 ZEÚ založená (pozri v tomto zmysle rozsudky z 12. júna 2003, Schmidberger, C-112/00, EU:C:2003:333, bod 79, a zo 6. septembra 2011, Patriciello, C-163/10, EU:C:2011:543, bod 31).
- 94 V tejto súvislosti treba pripomenúť, že v súlade s článkom 52 ods. 1 Charty akékoľvek obmedzenie výkonu práv a slobôd uznaných v Charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných (rozsudok z 15. februára 2016, N., C-601/15 PPU, EU:C:2016:84, bod 50).

- 95 V tejto súvislosti článok 15 ods. 1 prvá veta smernice 2002/58 stanovuje, že členské štáty môžu prijať opatrenie, ktoré predstavuje výnimku zo zásady dôvernosti údajov o prenose dát súvisiacich s elektronickými komunikáciami, ak ide o „nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti“, so zreteľom na ciele, ktoré toto ustanovenie stanovuje. Pokiaľ ide o odôvodnenie 11 tejto smernice, toto odôvodnenie spresňuje, že opatrenie tohto druhu musí byť „prísne“ proporcionálne vo vzťahu k zamýšľanému účelu. Pokiaľ ide konkrétne o uchovávanie údajov, podľa článku 15 ods. 1 druhej vety uvedenej smernice sa vyžaduje, aby sa uskutočňovalo len „na limitované obdobie“ a pokiaľ je to „oprávnené“ jedným z cieľov uvedených v článku 15 ods. 1 prvej vete tejto istej smernice.
- 96 Dodržiavanie zásady proporcionality takisto vyplýva z ustálenej judikatúry Súdneho dvora, podľa ktorej ochrana základného práva na rešpektovanie súkromného života na úrovni Únie vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné (rozsudky zo 16. decembra 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727, bod 56; z 9. novembra 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662, bod 77; Digital Rights, bod 52, ako aj zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 92).
- 97 Pokiaľ ide o otázku, či taká vnútroštátna právna úprava, o akú ide vo veci C-203/15, spĺňa uvedené podmienky, treba uviesť, že táto právna úprava stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie, a vyžaduje od poskytovateľov elektronických komunikačných služieb uchovávať tieto údaje priebežne a systematicky, a to bez výnimky. Ako vyplýva z rozhodnutia vnútroštátneho súdu, kategórie údajov uvedené v tejto právnej úprave zodpovedajú v podstate tým, ktorých uchovávanie sa vyžadovalo podľa smernice 2006/24.
- 98 Údaje, ktoré teda musia uchovávať poskytovatelia elektronických komunikačných služieb, umožňujú zistenie a identifikáciu zdroja komunikácie a adresáta komunikácie, určenie dátumu, času, trvania a typu komunikácie, identifikáciu komunikačného zariadenia užívateľa, ako aj určenie polohy mobilného komunikačného zariadenia. Medzi tieto údaje patrí najmä meno a adresa účastníka alebo registrovaného užívateľa, telefónne číslo volajúceho a číslo volaného, ako aj IP adresa pre internetové služby. Z týchto údajov predovšetkým vyplýva, s kým a akým spôsobom účastník alebo registrovaný užívateľ komunikoval, ako aj čas komunikácie a miesto, z ktorého prebiehala. Okrem toho tieto údaje umožňujú zistiť, ako často účastník alebo registrovaný užívateľ komunikoval s určitými osobami v danom období (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 26).
- 99 Zo všetkých týchto údajov možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 27). Konkrétne takéto údaje poskytujú prostriedky na stanovenie – ako uviedol generálny advokát v bodoch 253, 254 a 257 až 259 svojich návrhov – profilu dotknutých osôb, čo je rovnako citlivá informácia, pokiaľ ide o právo na rešpektovanie súkromného života, ako samotný obsah komunikácií.
- 100 Zásah, ktorý spôsobuje takáto právna úprava do základných práv zakotvených v článkoch 7 a 8 Charty, sa javí ako rozsiahly a treba ho považovať za zvlášť závažný. Okolnosť, že uchovávanie údajov sa uskutočňuje bez toho, aby používatelia elektronických komunikačných služieb boli o tom informovaní, môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 37).
- 101 Napriek tomu, že taká právna úprava neumožňuje uchovávať obsah komunikácie, a teda nemôže zasiahnuť do podstaty základného práva na ochranu osobných údajov (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 39), uchovávanie údajov o prenose dát a polohe

môže mať vplyv na použitie elektronických komunikačných prostriedkov, a v dôsledku toho na výkon slobody prejavu zaručenej v článku 11 Charty používateľmi týchto elektronických prostriedkov (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 28).

- 102 Vzhľadom na závažnosť zásahu do predmetných základných práv, ktorý predstavuje vnútroštátna právna úprava, ktorá na účely boja proti trestnej činnosti stanovuje uchovávanie údajov o prenose dát a polohe, takéto opatrenie možno odôvodniť výhradne bojom proti závažnej trestnej činnosti (pozri analogicky v súvislosti so smernicou 2006/24 rozsudok Digital Rights, bod 60).
- 103 Okrem toho, hoci účinnosť boja proti závažnej trestnej činnosti, najmä proti organizovanému zločinu a terorizmu, môže do veľkej miery závisieť od použitia moderných vyšetrovacích technológií, takýto cieľ všeobecného záujmu, nech je akokoľvek zásadný, nemôže sám osebe odôvodniť to, aby sa vnútroštátna právna úprava, ktorá stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe, považovala za nevyhnutnú na účely uvedeného boja (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 51).
- 104 V tejto súvislosti treba na jednej strane uviesť, že vzhľadom na vlastnosti takejto právnej úpravy opísané v bode 97 tohto rozsudku je jej účinkom, že uchovávanie údajov o prenose dát a polohe predstavuje pravidlo, zatiaľ čo podľa systému zavedeného smernicou 2002/58 sa vyžaduje, aby uchovávanie údajov bolo výnimkou.
- 105 Na druhej strane vnútroštátna právna úprava, akou je právna úprava vo veci samej, ktorá všeobecne zahŕňa všetkých účastníkov a registrovaných užívateľov a všetky spôsoby elektronickej komunikácie, ako aj všetky údaje o prenose dát, nestanovuje žiadne rozlíšenie, obmedzenie alebo výnimku na základe sledovaného cieľa. Globálne sa týka všetkých osôb používajúcich elektronické komunikačné služby bez toho, aby sa tieto osoby aspoň nepriamo nachádzali v situácii, ktorá by mohla viesť k trestnému stíhaniu. Uplatňuje sa teda aj na osoby, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť so závažnými trestnými činmi. Navyše nestanovuje žiadnu výnimku, takže sa uplatňuje aj na osoby, ktorých komunikácia podľa pravidiel vnútroštátneho práva podlieha služobnému tajomstvu (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, body 57 a 58).
- 106 Takáto úprava nevyžaduje nijakú súvislosť medzi údajmi, ktorých uchovávanie stanovuje, a hrozbou pre verejnú bezpečnosť. Predovšetkým nie je obmedzená na uchovávanie, ktoré by sa vzťahovalo na údaje z určitého časového obdobia a/alebo z určitej zemepisnej oblasti a/alebo na okruh osôb, ktorý by akýmkoľvek spôsobom bolo možné spájať so závažnými trestnými činmi, ani na osoby, ktorých uchovávané údaje by z iných dôvodov mohli prispieť k boju proti trestnej činnosti (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 59).
- 107 Taká vnútroštátna právna úprava, o akú ide vo veci samej, ide nad rámec toho, čo je prísne nevyhnutné, a nemožno ju teda považovať za odôvodnenú v demokratickej spoločnosti, ako to vyžaduje článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty.
- 108 Na druhej strane článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty nebráni tomu, aby členský štát prijal právnu úpravu, ktorá preventívne umožňuje, aby sa cielene uchovávali údaje o prenose dát a polohe na účely boja proti závažnej trestnej činnosti pod podmienkou, že uchovávanie údajov bude, pokiaľ ide o kategórie uchovávaných údajov, príslušné komunikačné prostriedky, dotknuté osoby, ako aj dĺžku doby uchovávania, obmedzené na to, čo je prísne nevyhnutné.
- 109 Na splnenie požiadaviek uvedených v predchádzajúcom bode tohto rozsudku musí táto vnútroštátna právna úprava stanoviť v prvom rade jasné a presné pravidlá upravujúce rozsah a uplatnenie takeého opatrenia na uchovávanie údajov a ukládajúce minimálne požiadavky spôsobom, aby osoby, ktorých údaje boli uchované, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje pred

rizikami zneužitia. Táto právna úprava musí najmä uvádzať, za akých podmienok môže byť opatrenie na uchovávanie údajov preventívne prijaté, čím sa zabezpečí, že také opatrenie sa obmedzí na to, čo je prísne nevyhnutné (pozri analogicky v súvislosti so smernicou 2006/24, rozsudok Digital Rights, bod 54 a citovaných judikatúru).

- 110 Po druhé, čo sa týka hmotnoprávných podmienok, ktoré musí spĺňať vnútroštátna právna úprava, ktorá v rámci boja proti trestnej činnosti umožňuje preventívne uchovávanie údajov o prenose dát a polohe s cieľom zabezpečiť, aby sa uchovávanie obmedzilo na to, čo je prísne nevyhnutné, treba uviesť, že hoci sa tieto podmienky môžu značne líšiť v závislosti od opatrení prijatých na účely predchádzania trestným činom, vyšetrovania, odhaľovania a stíhania závažnej trestnej činnosti, musí uchovávanie údajov vždy zodpovedať objektívnym kritériám, ktoré zodpovedajú vzťahu medzi uchovávanými údajmi a sledovaným cieľom. Takéto podmienky sa musia konkrétne v praxi ukázať ako spôsobilé vymedziť rozsah opatrenia a v dôsledku toho aj dotknutú verejnosť.
- 111 Pokiaľ ide o vymedzenie takéhoto opatrenia s ohľadom na verejnosť a potenciálne dotknuté situácie, vnútroštátna právna úprava sa musí zakladať na objektívnych skutočnostiach, ktoré umožňujú definovať určitý okruh osôb z radov verejnosti, ktorých údaje môžu aspoň nepriamo súvisieť so závažnou trestnou činnosťou, podporiť určitým spôsobom boj proti závažnej trestnej činnosti alebo zabrániť vážnemu ohrozeniu verejnej bezpečnosti. Takéto vymedzenie možno zabezpečiť prostredníctvom geografického kritéria, pokiaľ sa príslušné vnútroštátne orgány na základe objektívnych skutočností domnievajú, že existuje v jednej alebo viacerých zemepisných oblastiach vysoké riziko prípravy alebo páchania takých činov.
- 112 Vzhľadom na všetky vyššie uvedené úvahy treba na prvú otázku vo veci C-203/15 odpovedať, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá na účely boja proti trestnej činnosti stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie.

O druhej otázke vo veci C-203/15 a prvej otázke vo veci C-698/15

- 113 Treba uviesť, že Kamarrätten i Stockholm (Odvolací správny súd Štokholm) položil druhú otázku vo veci C-203/15 len pre prípad zápornej odpovede na prvú otázku v uvedenej veci. Táto druhá otázka však nesúvisí so všeobecným alebo cieľovým charakterom uchovávania údajov v zmysle uvedenom v bodoch 108 až 111 tohto rozsudku. Preto treba spoločne odpovedať na druhú otázku vo veci C-203/15 a prvú otázku vo veci C-698/15, ktorá bola položená nezávisle od rozsahu povinnosti uchovávania údajov uloženej poskytovateľom elektronických komunikačných služieb.
- 114 Druhou otázkou vo veci C-203/15 a prvou otázkou vo veci C-698/15 sa vnútroštátne súdy v podstate pýtajú, či sa má článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7 a 8, ako aj s článkom 52 ods. 1 Charty vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá upravuje ochranu a bezpečnosť údajov o prenose dát a polohe, konkrétne prístup príslušných vnútroštátnych orgánov k uchovávaným údajom, ale tento prístup neobmedzuje len na účely boja proti závažnej trestnej činnosti, nepodmieňuje uvedený prístup predbežným preskúmaním zo strany súdu alebo nezávislého správneho orgánu, a nevyžaduje, že predmetné údaje sa musia uchovávať na území Únie.
- 115 Pokiaľ ide o ciele, ktoré môžu odôvodňovať vnútroštátnu právnu úpravu odchyľujúcu sa od zásady dôvernosti elektronických komunikácií, treba pripomenúť, že – ako sa konštatovalo v bodoch 90 a 102 tohto rozsudku – keďže výpočet cieľov uvedených v článku 15 ods. 1 prvej vete smernice 2002/58 je taxatívny, prístup k uchovávaným údajom musí skutočne a výlučne zodpovedať jednému z týchto cieľov. Okrem toho, keďže cieľ sledovaný touto právnu úpravou musí byť priamo úmerný závažnosti

zásahu do základných práv, ktoré má tento prístup, vyplýva z toho, že v oblasti prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, jedine boj proti závažnej trestnej činnosti môže odôvodniť takýto prístup k uchovávaným údajom.

- 116 Pokiaľ ide o dodržanie zásady proporcionality, vnútroštátna právna úprava upravujúca podmienky, za akých musia poskytovatelia elektronických komunikačných služieb poskytnúť prístup príslušným vnútroštátnym orgánom k uchovávaným údajom, musí zabezpečiť, ako sa konštatovalo v bodoch 95 a 96 tohto rozsudku, že takýto prístup sa poskytne len v rámci toho, čo je prísne nevyhnutné.
- 117 Okrem toho, keďže legislatívne opatrenia uvedené v článku 15 ods. 1 smernice 2002/58 majú podľa odôvodnenia 11 tejto smernice „byť predmetom primeranej ochrany“, takéto opatrenie musí, ako vyplýva z judikatúry citovanej v bode 109 tohto rozsudku, stanoviť jasné a presné pravidlá uvádzajúce, za akých okolností a podmienok musia poskytovatelia elektronických komunikačných služieb poskytnúť prístup príslušným vnútroštátnym orgánom k uchovávaným údajom. Okrem toho takéto opatrenie musí byť podľa vnútroštátneho práva právne záväzné.
- 118 S cieľom zabezpečiť, aby sa prístup príslušných vnútroštátnych orgánov k uchovávaným údajom obmedzoval na to, čo je prísne nevyhnutné, samozrejme prináleží vnútroštátnemu právu, aby sa ním určili podmienky, za akých poskytovatelia elektronických komunikačných služieb majú takýto prístup poskytnúť. V prípade dotknutej vnútroštátnej právnej úpravy však nestačí, aby vyžadovala len to, že prístup musí zodpovedať niektorému z cieľov uvedených v článku 15 ods. 1 smernice 2002/58, aj keby išlo o boj proti závažnej trestnej činnosti. Taká vnútroštátna právna úprava musí totiž upravovať aj hmotnoprávne a procesnoprávne podmienky prístupu príslušných vnútroštátnych orgánov k uchovávaným údajom (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 61).
- 119 Keďže všeobecný prístup ku všetkým uchovávaným údajom, bez ohľadu na akúkoľvek spojitosť – čo i len nepriamu – so sledovaným účelom nemožno považovať za obmedzený na prísne nevyhnutné, dotknutá vnútroštátna právna úprava sa musí zakladať na objektívnych kritériách s cieľom určiť okolnosti a podmienky, za akých sa má poskytnúť prístup príslušným vnútroštátnym orgánom k uchovávaným údajom účastníkov alebo registrovaných užívateľov. Z tohto pohľadu možno taký prístup v súvislosti s cieľom boja proti kriminalite v zásade poskytnúť len k údajom osôb podozrivých z prípravy, páchania alebo zo spáchania závažného trestného činu, ako aj tých, ktoré sa takým či onakým spôsobom podieľali na takom trestnom čine (pozri analogicky rozhodnutie ESLP zo 4. decembra 2015, Roman Zacharov v. Rusko, CE:ECHR:2015:1204JUD004714306, § 260). Za osobitných okolností, ako sú okolnosti, za akých životne dôležité záujmy národnej bezpečnosti, obrany alebo verejnej bezpečnosti sú ohrozené teroristickými aktivitami, možno však poskytnúť prístup aj k údajom iných osôb, pokiaľ existujú objektívne skutočnosti, na základe ktorých sa možno domnievať, že tieto údaje môžu v konkrétnom prípade účinne prispieť k boju proti takýmto činnostiam.
- 120 S cieľom zabezpečiť v praxi úplné dodržiavanie týchto podmienok je nevyhnutné, aby prístup príslušných vnútroštátnych orgánov k uchovávaným údajom podliehal v zásade – s výnimkou riadne odôvodnených naliehavých prípadov – predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a aby rozhodnutie tohto súdu alebo orgánu nasledovalo po odôvodnenej žiadosti týchto orgánov podanej v rámci konania týkajúceho sa predchádzania trestným činom, ich odhaľovania a stíhania (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, bod 62; pozri tiež analogicky, pokiaľ ide o článok 8 EDLP, rozhodnutie ESLP z 12. januára 2016, Szabó a Vissy v. Maďarsko CE:ECHR:2016:0112JUD003713814, § 77 a § 80).
- 121 Rovnako dôležité je aj to, aby príslušné vnútroštátne orgány, ktorým bol udelený prístup k uchovávaným údajom, informovali dotknuté osoby v rámci uplatniteľných vnútroštátnych konaní od okamihu, keď toto oznámenie nemôže ohroziť vyšetrovanie týchto orgánov. Táto informácia je totiž pre tieto osoby *de facto* nevyhnutná na to, aby mohli vykonať najmä svoje právo na opravný prostriedok

výslovne stanovený v článku 15 ods. 2 smernice 2002/58 v spojení s článkom 22 smernice 95/46 v prípade, že ich práva boli porušené (pozri analogicky rozsudky zo 7. mája 2009, Rijkeboer, C-553/07, EU:C:2009:293, bod 52, ako aj zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, bod 95).

- 122 Pokiaľ ide o pravidlá týkajúce sa bezpečnosti a ochrany údajov uchovávaných poskytovateľmi elektronických komunikačných služieb, treba konštatovať, že článok 15 ods. 1 smernice 2002/58 neumožňuje členským štátom odchýliť sa od článku 4 ods. 1, ani od článku 4 ods. 1a tejto smernice. Tieto ustanovenia vyžadujú, aby uvedení poskytovatelia prijali vhodné technické a organizačné opatrenia na zabezpečenie účinnej ochrany uchovávaných údajov pred rizikom zneužitia, ako aj pred akýmkoľvek nezákonným prístupom k týmto údajom. Vzhľadom na množstvo uchovávaných údajov, citlivú povahu týchto údajov, ako aj riziko nezákonného prístupu k nim musia poskytovatelia elektronických komunikačných služieb na účely zaistenia úplnej integrity a dôvernosti týchto údajov zaručovať veľmi vysokú úroveň ochrany a bezpečnosti prostredníctvom primeraných technických a organizačných opatrení. Vnútroštátna právna úprava musí konkrétne stanovovať uchovávanie údajov na území Únie, ako aj nenávratné zničenie údajov po skončení doby ich uchovávaní (pozri analogicky, pokiaľ ide o smernicu 2006/24, rozsudok Digital Rights, body 66 až 68).
- 123 V každom prípade členské štáty musia zabezpečiť, že nezávislý orgán bude vykonávať kontrolu dodržiavania úrovne ochrany zaručenej právom Únie v oblasti ochrany fyzických osôb pri spracovaní osobných údajov, pretože taká kontrola sa výslovne vyžaduje podľa článku 8 ods. 3 Charty a v súlade s ustálenou judikatúrou Súdneho dvora predstavuje základný prvok rešpektovania ochrany osôb, pokiaľ ide o spracovávanie osobných údajov. V opačnom prípade by osoby, ktorých osobné údaje sa uchovávajú, boli zbavené práva zaručeného článkom 8 ods. 1 a 3 Charty, podľa ktorého môžu podať na vnútroštátne dozorné orgány žiadosť na účely ochrany ich údajov (pozri v tomto zmysle rozsudky Digital Rights, bod 68, ako aj zo 6. októbra 2015, Schrems, C-362/14, EU:C:2015:650, body 41 a 58).
- 124 Vnútroštátnym súdom prináleží overiť, či a v akom rozsahu vnútroštátne právne úpravy, o ktoré ide vo veci samej, dodržiavajú požiadavky vyplývajúce z článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, ako boli spresnené v bodoch 115 až 123 tohto rozsudku, tak pokiaľ ide o poskytnutie prístupu príslušným vnútroštátnym orgánom k uchovávaným údajom, ako aj o ochranu a úroveň bezpečnosti týchto údajov.
- 125 Vzhľadom na všetky vyššie uvedené úvahy treba na druhú otázku vo veci C-203/15 a prvú otázku vo veci C-698/15 odpovedať, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá upravuje ochranu a bezpečnosť údajov o prenose dát a polohe, konkrétne prístup príslušných vnútroštátnych orgánov k uchovávaným údajom, ale tento prístup v rámci boja proti trestnej činnosti neobmedzuje len na účely boja proti závažnej trestnej činnosti, nepodmieňuje uvedený prístup predbežnému preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a nevyžaduje, že predmetné údaje sa musia uchovávať na území Únie.

O druhej otázke vo veci C-698/15

- 126 Druhou otázkou vo veci C-698/15 sa Court of Appeal (England & Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát)] v podstate pýta, či v rozsudku Digital Rights Súdny dvor vyložil články 7 a/alebo 8 Charty v zmysle, ktorý ide nad rámec významu priznaného článku 8 EDLP Európskym súdom pre ľudské práva.
- 127 Na úvod treba pripomenúť, že hoci – ako potvrdzuje článok 6 ods. 3 ZEÚ – základné práva zaručené EDLP sú ako všeobecné zásady súčasťou práva Únie, tento dohovor, kým k nemu Únia nepristúpila, nepredstavuje právny nástroj formálne začlenený do právneho poriadku Únie (pozri v tomto zmysle rozsudok z 15. februára 2016, N., C-601/15 PPU, EU:C:2016:84, bod 45 a citovanú judikatúru).

- 128 Výklad smernice 2002/58, o ktorý ide v tomto prípade, treba preskúmať len s ohľadom na základné práva zaručené Chartou (pozri v tomto zmysle rozsudok z 15. februára 2016, N., C-601/15 PPU, EU:C:2016:84, bod 46 a citovanú judikatúru).
- 129 Navyše treba pripomenúť, že vo vysvetlivkách k článku 52 Charty sa uvádza, že cieľom odseku 3 tohto článku je zabezpečiť potrebnú súdržnosť medzi Chartou a EDLP „bez toho, aby tým bola narušená autonómia práva Únie a Súdneho dvora Európskej únie“ (rozsudok z 15. februára 2016, N., C-601/15 PPU, EU:C:2016:84, bod 47). Predovšetkým, ako výslovne stanovuje článok 52 ods. 3 druhá veta Charty, článok 52 ods. 3 prvá veta tejto Charty nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany ako EDLP. K tomu sa napokon pridáva skutočnosť, že článok 8 Charty sa týka základného práva odlišného od toho, ktoré je zakotvené v článku 7 tejto Charty a ktoré nemá ekvivalent v EDLP.
- 130 Podľa ustálenej judikatúry Súdneho dvora však návrh na začatie prejudiciálneho konania nesmie smerovať k formulovaniu poradných stanovísk o všeobecných alebo hypotetických otázkach, ale musí byť odôvodnený potrebou spojenou s účinným vyriešením sporu týkajúceho sa práva Únie (pozri v tomto zmysle rozsudky z 24. apríla 2012, Kamberaj, C-571/10, EU:C:2012:233, bod 41; z 26. februára 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, bod 42, ako aj z 27. februára 2014, Pohotovosť, C-470/12, EU:C:2014:101, bod 29).
- 131 V prejednávanej veci vzhľadom na úvahy uvedené najmä v bodoch 128 a 129 tohto rozsudku nemôže mať otázka, či ochrana priznaná článkami 7 a 8 Charty ide nad rámec toho, čo je zaručené článkom 8 EDLP, vplyv na výklad smernice 2002/58 v spojení s Chartou, ktorý je predmetom sporu vo veci samej vo veci C-698/15.
- 132 Preto sa nezdá, že by odpoveď na druhú otázku vo veci C-689/15 mohla poskytnúť výkladové prvky práva Únie, ktoré by boli nevyhnutné na rozhodnutie daného sporu z hľadiska tohto práva.
- 133 Z toho vyplýva že druhá otázka vo veci C-698/15 je neprípustná.

O trovách

- 134 Vzhľadom na to, že konanie pred Súdnym dvorom má vo vzťahu k účastníkom konania vo veci samej incidenčný charakter a bolo začaté v súvislosti s prekážkou postupu v konaní pred vnútroštátnymi súdmi, o trovách konania rozhodnú tieto vnútroštátne súdy. Iné trovy konania, ktoré vznikli v súvislosti s predložením pripomienok Súdnemu dvoru a nie sú trovami uvedených účastníkov konania, nemôžu byť nahradené.

Z týchto dôvodov Súdny dvor (veľká komora) rozhodol takto:

1. Článok 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenenej a doplnenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv Európskej únie sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá na účely boja proti trestnej činnosti stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie.
2. Článok 15 ods. 1 smernice 2002/58, zmenenej a doplnenej smernicou 2009/136, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá upravuje ochranu a bezpečnosť údajov o prenose dát a polohe, konkrétne prístup príslušných vnútroštátnych orgánov

k uchovávaným údajom, ale tento prístup v rámci boja proti trestnej činnosti neobmedzuje len na účely boja proti závažnej trestnej činnosti, nepodmieňuje uvedený prístup predbežnému preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a nevyžaduje, že predmetné údaje sa musia uchovávať na území Únie.

- 3. Druhá otázka, ktorú položil Court of Appeal (England & Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát), Spojené kráľovstvo] je neprípustná.**

Podpisy