Zbierka súdnych rozhodnutí

ROZSUDOK SÚDNEHO DVORA (veľká komora)

zo 6. októbra 2020*

„Návrh na začatie prejudiciálneho konania – Spracovávanie osobných údajov v sektore elektronických komunikácií – Poskytovatelia elektronických komunikačných služieb – Všeobecné a nediferencované odovzdávanie údajov o prenose dát a polohe – Ochrana národnej bezpečnosti – Smernica 2002/58/ES – Pôsobnosť – Článok 1 ods. 3 a článok 3 – Dôvernosť elektronickej komunikácie – Ochrana – Článok 5 a článok 15 ods. 1 – Charta základných práv Európskej únie – Články 7, 8 a 11, ako aj článok 52 ods. 1 – Článok 4 ods. 2 ZEÚ“

Vo veci C-623/17,

ktorej predmetom je návrh na začatie prejudiciálneho konania podľa článku 267 ZFEÚ, podaný rozhodnutím Investigatory Powers Tribunal (Súd pre kontrolu vyšetrovacích právomocí, Spojené kráľovstvo) z 18. októbra 2017 a doručený Súdnemu dvoru 31. októbra 2017, ktorý súvisí s konaním:

Privacy International

proti

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

SÚDNY DVOR (veľká komora),

v zložení: predseda K. Lenaerts, podpredsedníčka R. Silva de Lapuerta, predsedovia komôr J.-C. Bonichot, A. Arabadžiev, A. Prechal, M. Safjan, P. G. Xuereb a L. S. Rossi, sudcovia J. Malenovský, L. Bay Larsen, T. von Danwitz (spravodajca), C. Toader, K. Jürimäe, C. Lycourgos a N. Piçarra,

generálny advokát: M. Campos Sánchez-Bordona,

tajomník: C. Strömholm, referentka,

so zreteľom na písomnú časť konania a po pojednávaní z 9. a 10. septembra 2019,

* Jazyk konania: angličtina.

so zreteľom na pripomienky, ktoré predložili:

– Privacy International, v zastúpení: B. Jaffey a T. de la Mare, QC, D. Cashman, solicitor, a H. Roy, avocat,

– vláda Spojeného kráľovstva, v zastúpení: Z. Lavery, D. Guðmundsdóttir a S. Brandon, splnomocnení zástupcovia, za právnej pomoci G. Facenna a D. Beard, QC, a C. Knight a R. Palmer, barristers,

– belgická vláda, v zastúpení: P. Cottin a J.-C. Halleux, splnomocnení zástupcovia, za právnej pomoci J. Vanpraet, advocaat, a E. de Lophem, avocat,

– česká vláda, v zastúpení: M. Smolek, J. Vláčil a O. Serdula, splnomocnení zástupcovia,

– nemecká vláda, v zastúpení: pôvodne M. Hellmann, R. Kanitz, D. Klebs a T. Henze, neskôr J. Möller, M. Hellmann, R. Kanitz a D. Klebs, splnomocnení zástupcovia,

– estónska vláda, v zastúpení: A. Kalbus, splnomocnená zástupkyňa,

– írska vláda, v zastúpení: M. Browne, G. Hodge a A. Joyce, splnomocnení zástupcovia, za právnej pomoci D. Fennelly, barrister,

– španielska vláda, v zastúpení: pôvodne L. Aguilera Ruiz a J. García-Valdecasas Dorrego, neskôr L. Aguilera Ruiz, splnomocnení zástupcovia,

– francúzska vláda, v zastúpení: pôvodne E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas a D. Dubois, neskôr E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune a D. Dubois, splnomocnení zástupcovia,

– cyperská vláda, v zastúpení: E. Symeonidou a E. Neofytou, splnomocnené zástupkyne,

– lotyšská vláda, v zastúpení: pôvodne V. Soņeca a I. Kucina, neskôr V. Soņeca, splnomocnené zástupkyne,

– maďarská vláda, v zastúpení: pôvodne G. Koós, M. Z. Fehér, G. Tornyai a Z. Wagner, neskôr G. Koós a M. Z. Fehér, splnomocnení zástupcovia,

– holandská vláda, v zastúpení: C. S. Schillemans a M. K. Bulterman, splnomocnené zástupkyne,

– poľská vláda, v zastúpení: B. Majczyna, J. Sawicka a M. Pawlicka, splnomocnení zástupcovia,

– portugalská vláda, v zastúpení: L. Inez Fernandes, M. Figueiredo a F. Aragão Homem, splnomocnení zástupcovia,

– švédska vláda, v zastúpení: pôvodne A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren a A. Alriksson, neskôr H. Shev, C. Meyer-Seitz, L. Zettergren a A. Alriksson, splnomocnené zástupkyne,

– nórska vláda, v zastúpení: T. B. Leming, M. Emberland a J. Vangsnes, splnomocnení zástupcovia,

– Európska komisia, v zastúpení: pôvodne H. Kranenborg, M. Wasmeier, D. Nardi a P. Costa de Oliveira, neskôr H. Kranenborg, M. Wasmeier a D. Nardi, splnomocnení zástupcovia,

– Európsky dozorný úradník pre ochranu údajov, v zastúpení: T. Zerdick a A. Buchta, splnomocnení zástupcovia,

po vypočutí návrhov generálneho advokáta na pojednávaní 15. januára 2020,

vyhlásil tento

Rozsudok

1 Návrh na začatie prejudiciálneho konania sa týka výkladu článku 1 ods. 3 a článku 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514), zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (Ú. v. EÚ L 337, 2009, s. 11) (ďalej len „smernica 2002/58“), v spojení s článkom 4 ods. 2 ZEÚ, ako aj s článkami 7, 8 a článkom 52 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“).

2 Tento návrh bol podaný v rámci sporu medzi organizáciou Privacy International na jednej strane a Secretary of State for Foreign and Commonwealth Affairs (minister zahraničných vecí a záležitostí Britského spoločenstva národov, Spojené kráľovstvo), Secretary of State for the Home Departement (minister vnútra, Spojené kráľovstvo), Government Communications Headquarters (Komunikačné ústredie vlády, Spojené kráľovstvo) (ďalej len „GCHQ“), Security Service (Bezpečnostná služba, Spojené kráľovstvo, ďalej len „MI5“) a Secret Intelligence Service (Tajná spravodajská služba, Spojené kráľovstvo, ďalej len „MI6“) na druhej strane v súvislosti so zákonnosťou právnej úpravy, ktorá bezpečnostným a spravodajským službám umožňuje získavať a využívať hromadné údaje o komunikácii *(bulk communications data)*.

Právny rámec

Právo Únie

Smernica 95/46

3 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, 1995, s. 31; Mim. vyd. 13/015, s. 355) bola s účinnosťou od 25. mája 2018 zrušená nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (Ú. v. EÚ L 119, 2016, s. 1). Článok 3 uvedenej smernice, nazvaný „Rozsah“, znel:

„1. Táto smernica sa uplatňuje na spracovanie osobných údajov vcelku alebo čiastočných údajov, automatickými prostriedkami, a na spracovanie osobných údajov inými, ako automatickými prostriedkami, ktoré tvoria časť registračného systému alebo určených pre to, aby tvorili časť registračného systému.

2. Táto smernica sa neuplatňuje na spracovanie osobných údajov:

– v priebehu činností, ktoré sú mimo rozsahu zákona [práva – *neoficiálny preklad*] spoločenstva, ako sú tie, ktoré sú uvedené v hlave V a VI [ZEÚ], a v žiadnom prípade sa neuplatňuj[e] na operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa operácia spracovania týka záležitostí bezpečnosti štátu) a činností štátu v oblastiach trestného zákona [práva – *neoficiálny preklad*],

– fyzickou osobou v priebehu osobnej činnosti, alebo činnosti týkajúcej sa domácnosti [fyzickou osobou na výkon výlučne osobných alebo domácich činností – *neoficiálny preklad*].“

Smernica 2002/58

4 Odôvodnenia 2, 6, 7, 11, 22, 26 a 30 smernice 2002/58 uvádzajú:

„(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 uvedenej charty.

…

(6) Internet revolucionalizoval 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 uchovávania a spracovávania údajov týkajúcich sa účastníkov a užívateľov.

…

(11) Podobne ako smernica [95/46] sa táto smernica netýka otázok ochrany základných práv a slobôd vzťahujúcich sa k činnostiam, ktoré nie sú upravené právom [Únie]. Preto nemení 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 [podpísaným v Ríme 4. novembra 1950], interpretovaným rozsudkami súdneho dvora týkajúcimi sa ľudských práv [Európskeho súdu pre ľudské práva – *neoficiálny preklad*]; 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.

…

(22) Zákaz ukladania správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] 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 dôvernosť informácií. Keď je to nevyhnutné z dôvodu efektívneho ďalšieho prenosu akýchkoľvek verejne dostupných informácií ostatných príjemcom služby na ich žiadosť, táto smernica by nemala brániť, aby boli také informácie ďalej uložené za predpokladu, že také informácie by v žiadnom prípade neboli dostupné pre verejnosť bez obmedzenia a že akékoľvek údaje týkajúce sa jednotlivých účastníkov alebo užívateľov požadujúcich také informácie by boli vymazané.

…

(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; prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] používané na marketingové komunikačné služby… by sa mali tiež vymazať alebo by mali byť anonymné…

…

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

5 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 [Európskej únii].

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 [ZFEÚ], 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 [činnosti štátu – *neoficiálny preklad*] v oblasti trestného práva.“

6 Článok 2 tejto smernice, nazvaný „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:

a) ‚užívateľ‘ znamená každú fyzickú osobu, ktorá používa verejne dostupnú elektronickú komunikačnú službu na súkromné alebo obchodné účely bez toho, aby si túto službu predplatil;

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;

…“

7 Článok 3 uvedenej smernice, 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 [Únii] vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu.“

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

„1. Členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí. Zakážu najmä počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami [príslušnými 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, nazvaný „Prevádzkové údaje [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 [anonymizovať – *neoficiálny preklad*], 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, nazvaný „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 používateľov 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 [údajov o polohe – *neoficiálny preklad*] 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]“, v odseku 1 uvádza:

„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 [neoprávneného používania – *neoficiálny preklad*] 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 [Únie] vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 Zmluvy o Európskej únii.“

Nariadenie 2016/679

12 Článok 2 nariadenia 2016/679 stanovuje:

„1. Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

2. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov:

a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;

b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;

…

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

…“

13 Článok 4 tohto nariadenia stanovuje:

„Na účely tohoto nariadenia:

…

2. ‚spracúvanie‘ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;

…“

14 Podľa článku 23 ods. 1 toho istého nariadenia:

„V práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť:

a) národnú bezpečnosť;

b) obranu;

c) verejnú bezpečnosť;

d) predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzanie;

e) iné dôležité ciele všeobecného verejného záujmu Únie alebo členského štátu, najmä predmet dôležitého hospodárskeho alebo finančného záujmu Únie alebo členského štátu vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia a sociálneho zabezpečenia;

f) ochranu nezávislosti súdnictva a súdnych konaní;

g) predchádzanie porušeniam etiky pre regulované profesie, ich vyšetrovanie, odhaľovanie a stíhanie;

h) monitorovaciu, kontrolnú alebo regulačnú funkciu spojenú, hoci aj príležitostne, s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g);

i) ochranu dotknutej osoby alebo práv a slobôd iných;

j) vymáhanie občianskoprávnych nárokov.“

15 Podľa článku 94 ods. 2 nariadenia 2016/679:

„Odkazy na zrušenú smernicu sa považujú za odkazy na toto nariadenie. Odkazy na Pracovnú skupinu pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov, zriadenú článkom 29 smernice [95/46], sa považujú za odkazy na Európsky výbor pre ochranu údajov zriadený týmto nariadením.“

Právo Spojeného kráľovstva

16 § 94 Telecommunications Act 1984 (zákon o telekomunikáciách z roku 1984) v znení uplatniteľnom na skutkové okolnosti vo veci samej (ďalej len „zákon z roku 1984“), nazvaný „Pokyny v záujme národnej bezpečnosti atď.“, stanovuje:

„(1) Minister môže po konzultácii s osobou, na ktorú sa vzťahuje tento paragraf, zadať tejto osobe všeobecné pokyny, ktoré minister považuje za potrebné v záujme národnej bezpečnosti alebo v záujme vzťahov s vládou určitej krajiny alebo územia mimo Spojeného kráľovstva.

(2) Ak považuje minister za potrebné postupovať týmto spôsobom v záujme národnej bezpečnosti alebo v záujme vzťahov s vládou určitej krajiny alebo územia mimo Spojeného kráľovstva, môže po konzultácii s osobou, na ktorú sa vzťahuje tento paragraf, zadať tejto osobe pokyny, ktorými ju vyzve, aby (v závislosti od okolností konkrétneho prípadu) vykonala alebo nevykonala určitý úkon špecifikovaný v pokynoch.

(2A) Minister môže vydať pokyny podľa odseku 1 alebo 2 len vtedy, ak sa domnieva, že konanie vyžadované pokynmi je primerané cieľu, ktorý sa má týmto konaním dosiahnuť.

(3) Osoba, na ktorú sa vzťahuje tento paragraf, musí vykonať každý pokyn, ktorý jej minister zadá podľa tohto paragrafu, a to bez ohľadu na akúkoľvek inú povinnosť, ktorá jej vyplýva z časti 1 alebo časti 2 kapitoly 1 Communications Act 2003 [(zákon o komunikáciách z roku 2003)], a v prípade pokynov zadaných poskytovateľovi verejnej elektronickej komunikačnej siete aj vtedy, keď sa ho uvedené pokyny týkajú v inom postavení než je postavenie poskytovateľa prístupu do takejto siete.

(4) Minister predloží každej z komôr Parlamentu kópiu všetkých pokynov vydaných podľa tohto paragrafu, pokiaľ sa nedomnieva, že zverejnenie uvedených pokynov by bolo v rozpore so záujmami národnej bezpečnosti alebo so záujmami vzťahov s vládou krajiny alebo územia mimo Spojeného kráľovstva alebo s obchodnými záujmami určitej osoby.

(5) Žiadna osoba nesmie sprístupniť ani byť na základe zákona či inak povinná sprístupniť akékoľvek informácie týkajúce sa opatrení prijatých na základe tohto paragrafu, ak jej minister oznámil, že podľa jeho názoru je sprístupnenie týchto informácií v rozpore so záujmami národnej bezpečnosti alebo so záujmami vzťahov s vládou určitej krajiny alebo územia mimo Spojeného kráľovstva alebo s obchodnými záujmami inej osoby.

…

(8) Tento paragraf sa vzťahuje na [Office of communications (OFCOM)] a na poskytovateľov verejných elektronických komunikačných sietí.“

17 § 21 ods. 4 a 6 Regulation of Investigatory Powers Act 2000 (zákon o úprave vyšetrovacích právomocí z roku 2000, ďalej len „RIPA“) stanovuje:

„(4) Pod pojmom ‚údaje týkajúce sa komunikácií‘ sa 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 nespadajú 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.

…

(6) Pojem ‚údaje o prenose dát‘ v súvislosti s akoukoľvek komunikáciou sa vzťahuje na:

a) akýkoľvek údaj, ktorý identifikuje alebo môže identifikovať akúkoľvek osobu, zariadenie alebo miesto, na ktoré alebo z ktorého sa komunikácia prenesie alebo môže preniesť;

b) akýkoľvek údaj, ktorý identifikuje alebo vyberie, alebo môže identifikovať alebo vybrať zariadenie, ktorým sa komunikácia prenesie alebo ktorým môže byť komunikácia prenesená;

c) akýkoľvek údaj, ktorý obsahuje signály na spustenie zariadenia použitého v komunikačnom systéme na účely prenosu akejkoľvek komunikácie, a

d) akýkoľvek údaj, ktorý identifikuje údaje zahrnuté alebo pripojené ku konkrétnej komunikácii alebo iné údaje, ktoré sú zahrnuté alebo pripojené ku konkrétnej komunikácii.

…“

18 § 65 až 69 RIPA stanovujú pravidlá týkajúce sa fungovania a právomocí Investigatory Powers Tribunal (Súd pre vyšetrovacie právomoci, Spojené kráľovstvo). Podľa § 65 tohto zákona, ak existuje dôvod domnievať sa, že údaje boli získané protiprávne, možno na tento súd podať sťažnosť.

Spor vo veci samej a prejudiciálne otázky

19 Začiatkom roka 2015 bola najmä v správe Intelligence and Security Committee of Parliament (Výbor Parlamentu pre bezpečnosť a spravodajskú činnosť, Spojené kráľovstvo) zverejnená informácia o praktikách zberu a využívania hromadných údajov o komunikáciách zo strany rôznych bezpečnostných a spravodajských služieb Spojeného kráľovstva, konkrétne GCHQ, MI5 a MI6. Dňa 5. júna 2015 podala mimovládna organizácia Privacy International proti ministrovi zahraničných vecí a záležitostí Britského spoločenstva národov, ministrovi vnútra, ako aj týmto bezpečnostným a spravodajským službám žalobu na Investigatory Powers Tribunal (Súd pre vyšetrovacie právomoci, Spojené kráľovstvo), ktorou spochybňuje zákonnosť týchto postupov.

20 Vnútroštátny súd preskúmal zákonnosť uvedených postupov najskôr z hľadiska vnútroštátneho práva a ustanovení Európskeho dohovoru o ochrane ľudských práv a základných slobôd, podpísaného v Ríme 4. novembra 1950 (ďalej len „EDĽP“), a následne z hľadiska práva Únie. V rozsudku zo 17. októbra 2016 tento súd konštatoval, že žalovaní vo veci samej uznali, že uvedené bezpečnostné a spravodajské služby v rámci svojich činností zbierali a využívali súbory údajov o jednotlivcoch, ktoré patria do rôznych kategórií (*bulk personal data*), ako sú napríklad osobné údaje alebo údaje o cestovaní, informácie finančnej alebo obchodnej povahy, údaje súvisiace s komunikáciou, ktoré môžu zahŕňať citlivé údaje podliehajúce služobnému tajomstvu, alebo tiež podklady pre žurnalistiku. Tieto údaje, získané rôznymi spôsobmi, v prípade potreby aj tajne, sú analyzované ich porovnávaním alebo automatizovaným spracúvaním a môžu byť sprístupnené iným osobám a orgánom alebo zdieľané so zahraničnými partnermi. V tejto súvislosti bezpečnostné a spravodajské služby využívajú aj hromadné údaje o komunikáciách vyzbierané od poskytovateľov verejných elektronických komunikačných sietí najmä na základe pokynov ministerstva prijatých na základe § 94 zákona z roku 1984. GCHQ takto postupovala od roku 2001 a MI5 od roku 2005.

21 Uvedený súd dospel k záveru, že tieto opatrenia týkajúce sa zberu a využívania údajov boli v súlade s vnútroštátnym právom a od roku 2015 – s výhradou ešte neposúdených otázok v súvislosti s primeranosťou uvedených opatrení a prenosom údajov tretím stranám – s článkom 8 EDĽP. K tomuto poslednému uvedenému aspektu uviedol, že mu boli predložené dôkazy týkajúce sa príslušných záruk, najmä pokiaľ ide o procesy prístupu a zverejňovania mimo bezpečnostných a spravodajských služieb, spôsobov uchovávania údajov a existencie nezávislých kontrol.

22 Pokiaľ ide o zákonnosť opatrení týkajúcich sa zberu a využívania údajov, o ktoré ide vo veci samej, z hľadiska práva Únie, vnútroštátny súd v rozsudku z 8. septembra 2017 posudzoval, či tieto opatrenia patria do pôsobnosti práva Únie, a ak áno, či sú zlučiteľné s týmto právom. V súvislosti s hromadnými údajmi o komunikáciách tento súd konštatoval, že poskytovatelia elektronických komunikačných sietí boli na základe § 94 zákona z roku 1984 povinní v prípade, že minister vydal pokyny v príslušnom zmysle, poskytnúť bezpečnostným a spravodajským službám údaje zhromaždené v rámci svojej ekonomickej činnosti, na ktorú sa vzťahuje právo Únie. To však neplatilo pre zber iných údajov získavaných uvedenými službami bez využitia takýchto donucovacích právomocí. Na základe tohto konštatovania považoval tento súd za potrebné položiť Súdnemu dvoru otázku s cieľom určiť, či sa na taký režim, aký vyplýva z uvedeného § 94, vzťahuje právo Únie, a v prípade kladnej odpovede, či a akým spôsobom sa na tento režim uplatnia požiadavky stanovené judikatúrou vyplývajúcou z rozsudku z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, ďalej len „rozsudok Tele2“, EU:C:2016:970).

23 V tejto súvislosti vnútroštátny súd v návrhu na začatie prejudiciálneho konania uvádza, že podľa uvedeného § 94 môže minister zadávať poskytovateľom elektronických komunikačných služieb všeobecné alebo konkrétne pokyny, ktoré považuje za potrebné v záujme národnej bezpečnosti alebo v záujme vzťahov s cudzou vládou. S odkazom na definície obsiahnuté v § 21 ods. 4 a 6 RIPA tento súd spresňuje, že dotknuté údaje zahŕňajú údaje o prenose dát a informácie o použitých službách v zmysle tohto ustanovenia, pričom vylúčený je len obsah komunikácií. Z týchto údajov a informácií možno najmä zistiť „kto, kedy, kde a ako“ komunikoval. Tieto údaje sú odovzdávané bezpečnostným a spravodajským službám, ktoré ich uchovávajú na účely svojej činnosti.

24 Podľa uvedeného súdu sa režim dotknutý vo veci samej odlišuje od režimu, ktorý zaviedol Data Retention and Investigator Powers Act 2014 (zákon o uchovávaní údajov a vyšetrovacích právomociach z roku 2014) dotknutý vo veci, v ktorej bol vydaný rozsudok z 21. decembra 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970), pretože tento posledný uvedený režim stanovoval uchovávanie údajov poskytovateľmi elektronických komunikačných služieb a poskytovanie týchto údajov nielen bezpečnostným a spravodajským službám v záujme národnej bezpečnosti, ale tiež ďalším orgánom verejnej moci podľa ich potrieb. Tento rozsudok sa navyše týkal trestného vyšetrovania a nie národnej bezpečnosti.

25 Vnútroštátny súd dodáva, že databázy vytvorené bezpečnostnými a spravodajskými službami sú predmetom nešpecifického hromadného a automatizovaného spracovávania, ktorého účelom je odhaliť prípadné neznáme hrozby. K tomu tento súd uvádza, že takto vytvorené súbory metadát by mali byť čo najkomplexnejšie, aby bolo možné vytvoriť „kopu sena“, v ktorej treba nájsť „ihlu“, ktorá sa tam skrýva. V súvislosti s užitočnosťou hromadného zberu údajov uvedenými službami a metód vyhľadávania týchto údajov, uvedený súd odkazuje najmä na závery správy vypracovanej 19. augusta 2016 pánom Davidom Andersonom, QC, v tom čase United Kingdom Independent Reviewer of Terrorism Legislation (nezávislý kontrolór právnych predpisov Spojeného kráľovstva o terorizme), ktorý pri vypracovaní tejto správy vychádzal z analýzy uskutočnenej tímom odborníkov na spravodajstvo a z výpovedí príslušníkov bezpečnostných a spravodajských služieb.

26 Vnútroštátny súd tiež spresňuje, že podľa Privacy International je režim dotknutý vo veci samej z pohľadu práva Únie nezákonný, zatiaľ čo žalovaní vo veci samej sa domnievajú, že povinnosť odovzdávať údaje stanovená týmto režimom, prístup k týmto údajom a ani ich využitie nespadajú do právomocí Únie, a to najmä na základe článku 4 ods. 2 ZEÚ, podľa ktorého národná bezpečnosť ostáva vo výlučnej zodpovednosti každého členského štátu.

27 V tejto súvislosti vnútroštátny súd na základe rozsudku z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346, body 56 až 59), týkajúceho sa prenosu údajov PNR [*Passenger Name Records* (záznam podľa mena cestujúceho)] na účely ochrany verejnej bezpečnosti, zastáva názor, že činnosti obchodných spoločností v rámci spracúvania a prenosu údajov na účely ochrany národnej bezpečnosti zrejme nepatria do pôsobnosti práva Únie. Podľa tohto súdu sa netreba zaoberať otázkou, či predmetná činnosť predstavuje spracúvanie údajov, ale len otázkou, či je cieľom takejto činnosti z hľadiska jej podstaty a účinkov podpora niektorej zo základných funkcií štátu v zmysle článku 4 ods. 2 ZEÚ, a to prostredníctvom rámca stanoveného orgánmi verejnej moci v oblasti verejnej bezpečnosti.

28 Pokiaľ by sa však na opatrenia dotknuté vo veci samej vzťahovalo právo Únie, vnútroštátny súd zastáva názor, že požiadavky uvedené v bodoch 119 až 125 rozsudku z 21. decembra 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970), sa zdajú byť v kontexte národnej bezpečnosti neprimerané a mohli by oslabiť možnosti bezpečnostných a spravodajských služieb kontrolovať niektoré hrozby pre národnú bezpečnosť.

29 Za týchto okolností Investigatory Powers Tribunal (Súd pre vyšetrovacie právomoci) rozhodol prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:

„V prípade, keď:

a) možnosť [bezpečnostných a informačných služieb] využívať [hromadné údaje o komunikáciách], ktorá im bola poskytnutá, je nevyhnutná na ochranu národnej bezpečnosti Spojeného kráľovstva vrátane oblasti boja proti terorizmu, kontrašpionáže a boja proti šíreniu jadrových zbraní;

b) základným prvkom využívania [hromadných údajov o komunikáciách] zo strany [bezpečnostných a informačných služieb] je odhalenie predtým neznámych hrozieb pre národnú bezpečnosť prostredníctvom necielených hromadných techník, ktoré závisia od zhromažďovania hromadných údajov o komunikáciách na jednom mieste. Jeho hlavný prínos spočíva v rýchlej identifikácii a rýchlom vytvorení profilu cieľov, ako aj v opodstatnení konania v súvislosti s bezprostrednou hrozbou;

c) poskytovateľ elektronickej komunikačnej siete nie je následne povinný uchovávať [hromadné údaje o komunikáciách] (po uplynutí obdobia v súlade s jeho bežnými obchodnými požiadavkami), ktoré uchováva samotný štát ([bezpečnostnými a informačnými službami]);

d) vnútroštátny súd konštatoval (s výnimkou určitých vyhradených otázok), že záruky týkajúce sa využívania [hromadných údajov o komunikáciách] zo strany [bezpečnostných a informačných služieb] sú v súlade s požiadavkami EDĽP, a

e) vnútroštátny súd konštatoval, že uloženie požiadaviek uvedených v bodoch 119 až 125 rozsudku [z 21. decembra 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970)] by v prípade ich uplatnenia zmarilo opatrenia prijaté s cieľom zabezpečiť národnú bezpečnosť zo strany [bezpečnostných a informačných služieb] a v dôsledku toho by bola národná bezpečnosť Spojeného kráľovstva vystavená ohrozeniu;

1. Patrí požiadavka uvedená v pokynoch ministra, ktorá od poskytovateľa elektronickej komunikačnej siete požaduje dodanie hromadných údajov o komunikáciách bezpečnostným a spravodajským agentúram členského štátu, so zreteľom na článok 4 ZEÚ a článok 1 ods. 3 smernice 2002/58 do pôsobnosti práva Únie a smernice [2002/58]?

2. Ak je odpoveď na prvú otázku kladná, uplatňujú sa niektoré z požiadaviek [na uchovávané údaje o komunikáciách uvedené v bodoch 119 až 125 rozsudku z 21. decembra 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970)] alebo akékoľvek iné požiadavky okrem tých, ktoré ukladá EDĽP, na takýto pokyn ministra? Ak áno, ako a v akom rozsahu sa tieto požiadavky uplatňujú, vzhľadom na nevyhnutnosť potreby využívať metódy hromadného získavania a automatizovaného spracovania zo strany [bezpečnostných a informačných služieb] na ochranu národnej bezpečnosti a vzhľadom na rozsah, v akom môžu byť tieto možnosti, ak sú inak v súlade s EDĽP, zásadne oslabené zavedením takýchto požiadaviek?“

O prejudiciálnych otázkach

O prvej otázke

30 Svojou prvou otázkou sa vnútroštátny súd v podstate pýta, či sa má článok 1 ods. 3 smernice 2002/58 v spojení s článkom 4 ods. 2 ZEÚ vykladať v tom zmysle, že vnútroštátna právna úprava, ktorá umožňuje štátnemu orgánu uložiť poskytovateľom elektronických komunikačných služieb povinnosť odovzdávať bezpečnostným a spravodajským službám údaje o prenose dát a polohe na účely ochrany národnej bezpečnosti, patrí do pôsobnosti tejto smernice.

31 V tejto súvislosti Privacy International v podstate uvádza, že vzhľadom na poznatky vyplývajúce z judikatúry Súdneho dvora, pokiaľ ide o pôsobnosť smernice 2002/58, zber údajov bezpečnostnými a spravodajskými službami od týchto poskytovateľov na základe § 94 zákona z roku 1984, ako aj využívanie týchto údajov uvedenými službami patrí do pôsobnosti tejto smernice, či už sú uvedené údaje vyzbierané prostredníctvom odovzdania vykonaného po určitom čase alebo v reálnom čase. Konkrétne skutočnosť, že cieľ ochrany národnej bezpečnosti je výslovne uvedený v článku 15 ods. 1 uvedenej smernice, nemá za následok neuplatniteľnosť tejto smernice na takéto situácie a článok 4 ods. 2 ZEÚ nemá na toto posúdenie žiadny vplyv.

32 Naproti tomu vláda Spojeného kráľovstva, česká a estónska vláda, Írsko, ako aj francúzska, cyperská, maďarská, poľská a švédska vláda v podstate tvrdia, že smernica 2002/58 sa neuplatňuje na vnútroštátne právne predpisy dotknuté vo veci samej, keďže ich cieľom je ochrana národnej bezpečnosti. Činnosti bezpečnostných a spravodajských služieb sú súčasťou základných funkcií členských štátov, keďže sa týkajú udržiavania verejného poriadku, ako aj ochrany vnútornej bezpečnosti a územnej celistvosti, a v dôsledku toho patria do ich výlučnej právomoci, o čom svedčí najmä článok 4 ods. 2 tretia veta ZEÚ.

33 Smernicu 2002/58 preto podľa týchto vlád nemožno vykladať v tom zmysle, že vnútroštátne opatrenia na ochranu národnej bezpečnosti patria do jej pôsobnosti. Článok 1 ods. 3 tejto smernice obmedzuje rozsah jej pôsobnosti a vylučuje z nej činnosti týkajúce sa verejnej bezpečnosti, obrany a bezpečnosti štátu, ako to už v minulosti stanovil článok 3 ods. 2 prvá zarážka smernice 95/46. Tieto ustanovenia odrážajú rozdelenie právomocí stanovené v článku 4 ods. 2 ZEÚ a boli by zbavené potrebného účinku, ak by opatrenia v oblasti národnej bezpečnosti mali byť v súlade s požiadavkami smernice 2002/58. Okrem toho uvádzajú, že judikatúra Súdneho dvora zavedená rozsudkom z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346), týkajúcim sa článku 3 ods. 2 prvej zarážky smernice 95/46 je uplatniteľná na článok 1 ods. 3 smernice 2002/58.

34 V tomto smere treba uviesť, že 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 dôvernosť, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore.

35 Článok 1 ods. 3 tejto smernice vylučuje z jej pôsobnosti „činnosti štátu“ v oblastiach, ktoré sú v ňom vymenované, medzi ktorými sa nachádzajú činnosti štátu v oblasti trestného práva a činnosti týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu. Činnosti demonštratívne uvedené v tomto ustanovení sú v každom prípade činnosti patriace štátu alebo štátnym orgánom a nepatria do oblasti činností jednotlivcov (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 32 a citovaná judikatúra).

36 Článok 3 smernice 2002/58 ďalej uvádza, 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 (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 33 a citovaná judikatúra).

37 V tejto súvislosti 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“ (rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 71).

38 Článok 15 ods. 1 smernice 2002/58 nevyhnutne predpokladá, že v ňom uvedené vnútroštátne opatrenia patria do jej pôsobnosti, pretože táto smernica výslovne dovoľuje členským štátom prijať také opatrenia len v prípade splnenia podmienok, ktoré sú v nej stanovené. Okrem toho na účely uvedené v tomto ustanovení takéto opatrenia upravujú činnosť poskytovateľov elektronických komunikačných služieb (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 34 a citovaná judikatúra).

39 Súdny dvor najmä vzhľadom na tieto úvahy rozhodol, že článok 15 ods. 1 smernice 2002/58 v spojení s jej článkom 3 sa má vykladať v tom zmysle, že do pôsobnosti tejto smernice patrí nielen legislatívne opatrenie, ktoré poskytovateľom elektronických komunikačných služieb ukladá povinnosť uchovávať údaje o prenose dát a polohe, ale tiež legislatívne opatrenie, ktoré im ukladá povinnosť poskytnúť príslušným vnútroštátnym orgánom prístup k týmto údajom. Takéto legislatívne opatrenia totiž nevyhnutne zahŕňajú spracúvanie týchto údajov uvedenými poskytovateľmi a nemožno ich v rozsahu, v akom upravujú činnosti týchto poskytovateľov, zamieňať s činnosťami štátu uvedenými v článku 1 ods. 3 uvedenej smernice (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 35 a 37, ako aj citovanú judikatúru).

40 Pokiaľ ide o legislatívne opatrenie, akým je § 94 zákona z roku 1984, na základe ktorého môže príslušný orgán zadať poskytovateľom elektronických komunikačných služieb pokyn, aby poskytli hromadné údaje prenosom bezpečnostným a spravodajským službám, treba uviesť, že podľa definície uvedenej v článku 4 bode 2 nariadenia 2016/679, ktorá je uplatniteľná na základe článku 2 smernice 2002/58 v spojení s článkom 94 ods. 2 uvedeného nariadenia, pojem ‚spracúvanie osobných údajov' znamená „operáci[u] alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie,… uchovávanie,… prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom… bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami".

41 Z toho vyplýva, že poskytovanie osobných údajov prenosom predstavuje, rovnako ako uchovávanie údajov alebo akákoľvek iná forma sprístupnenia, spracúvanie v zmysle článku 3 smernice 2002/58 a v dôsledku toho patrí do pôsobnosti tejto smernice (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 45).

42 Okrem toho vzhľadom na úvahy uvedené v bode 38 tohto rozsudku a všeobecnú štruktúru smernice 2002/58 výklad tejto smernice, podľa ktorého sú legislatívne opatrenia uvedené v jej článku 15 ods. 1 vyňaté z pôsobnosti uvedenej smernice z dôvodu, že ciele, ktoré musia takéto opatrenia sledovať, sa výrazne prekrývajú s cieľmi sledovanými činnosťami uvedenými v článku 1 ods. 3 tej istej smernice, by zbavil článok 15 ods. 1 všetkého potrebného účinku (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 72 a 73).

43 Pojem „činnosti" uvedený v článku 1 ods. 3 smernice 2002/58 teda nemožno, ako v podstate uviedol generálny advokát v bode 75 svojich návrhov v spojených veciach La Quadrature du Net a i. (C-511/18 a C-512/18, EU:C:2020:6), na ktoré odkazuje v bode 24 svojich návrhov v prejednávanej veci, vykladať tak, že sa vzťahuje na legislatívne opatrenia uvedené v článku 15 ods. 1 tejto smernice.

44 Ustanovenia článku 4 ods. 2 ZEÚ, na ktoré odkazujú vlády uvedené v bode 32 tohto rozsudku, nemôžu tento záver vyvrátiť. Podľa ustálenej judikatúry Súdneho dvora, hoci členským štátom prináleží, aby vymedzili svoje hlavné bezpečnostné záujmy a prijali vhodné opatrenia na zaistenie svojej vnútornej a vonkajšej bezpečnosti, samotná skutočnosť, že určité vnútroštátne opatrenie je prijímané v záujme národnej bezpečnosti, nemôže viesť k tomu, že sa neuplatní právo Únie a členské štáty budú zbavené povinnosti nevyhnutne dodržiavať toto právo [pozri v tomto zmysle rozsudky zo 4. júna 2013, ZZ, C-300/11, EU:C:2013:363, bod 38 a citovanú judikatúru; z 20. marca 2018, Komisia/Rakúsko (Štátna tlačiareň), C-187/16, EU:C:2018:194, body 75 a 76, ako aj z 2. apríla 2020, Komisia/Poľsko, Maďarsko a Česká republika (Dočasný mechanizmus premiestnenia žiadateľov o medzinárodnú ochranu), C-715/17, C-718/17 a C-719/17, EU:C:2020:257, body 143 a 170].

45 Je pravda, že v rozsudku z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346, body 56 až 59), Súdny dvor rozhodol, že prenos osobných údajov leteckými spoločnosťami orgánom verejnej moci tretieho štátu na účely predchádzania terorizmu a iným závažným trestným činom a boja proti nim nepatrí podľa článku 3 ods. 2 prvej zarážky smernice 95/46 do pôsobnosti tejto smernice, pretože tento prenos patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti.

46 Vzhľadom na úvahy uvedené v bodoch 36, 38 a 39 tohto rozsudku však túto judikatúru nemožno uplatniť na výklad článku 1 ods. 3 smernice 2002/58. Ako v podstate uviedol generálny advokát v bodoch 70 až 72 svojich návrhov v spojených veciach La Quadrature du Net a i. (C-511/18 a C-512/18, EU:C:2020:6), článok 3 ods. 2 prvá zarážka smernice 95/46, ktorého sa týka uvedená judikatúra, totiž vo všeobecnosti vylučoval z pôsobnosti tejto poslednej uvedenej smernice „operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu", pričom sa nerozlišovali osoby, ktoré vykonávali dotknutú operáciu spracovania údajov. Naopak, v rámci výkladu článku 1 ods. 3 smernice 2002/58 sa takéto rozlišovanie javí ako nevyhnutné. Ako totiž vyplýva z bodov 37 až 39 a 42 tohto rozsudku, všetky operácie spracúvania osobných údajov vykonávané poskytovateľmi

elektronických komunikačných služieb patria do pôsobnosti uvedenej smernice, vrátane operácií spracúvania vyplývajúcich z povinností uložených týmto poskytovateľom zo strany orgánov verejnej moci, hoci sa na tieto posledné uvedené operácie spracúvania prípadne mohla vzťahovať výnimka stanovená v článku 3 ods. 2 prvej zarážke smernice 95/46 vzhľadom na širšiu formuláciu tohto ustanovenia, ktoré sa vzťahovalo na všetky operácie spracovania týkajúce sa verejnej bezpečnosti, obrany alebo bezpečnosti štátu, bez ohľadu na to, kto ich vykonával.

47 Okrem toho treba uviesť, že smernica 95/46, o ktorú ide vo veci, v ktorej bol vydaný rozsudok z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346), bola na základe článku 94 ods. 1 nariadenia 2016/679 zrušená a nahradená týmto nariadením, a to s účinnosťou od 25. mája 2018. Hoci uvedené nariadenie vo svojom článku 2 ods. 2 písm. d) spresňuje, že sa nevzťahuje na operácie spracovania vykonávané „príslušnými orgánmi“ najmä na účely predchádzania trestným činom a ich odhaľovania vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania, z článku 23 ods. 1 písm. d) a h) toho istého nariadenia vyplýva, že spracúvanie osobných údajov vykonávané jednotlivcami na rovnaké účely patrí do pôsobnosti tohto nariadenia. Z toho vyplýva, že vyššie uvedený výklad článku 1 ods. 3, článku 3 a článku 15 ods. 1 smernice 2002/58 je v súlade s vymedzením pôsobnosti nariadenia 2016/679, ktoré táto smernica dopĺňa a spresňuje.

48 Na druhej strane, ak členské štáty priamo vykonajú opatrenia, ktoré predstavujú výnimku zo zásady dôvernosti elektronických komunikácií, bez toho, aby ukladali povinnosť spracovávania poskytovateľom takýchto komunikačných služieb, na ochranu údajov dotknutých osôb sa nevzťahuje smernica 2002/58, ale len vnútroštátne právo, s výhradou uplatnenia smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89), takže dotknuté opatrenia musia byť v súlade najmä s vnútroštátnym ústavným právom a požiadavkami EDĽP.

49 Vzhľadom na predchádzajúce úvahy treba na prvú otázku odpovedať tak, že článok 1 ods. 3, článok 3 a článok 15 ods. 1 smernice 2002/58 v spojení s článkom 4 ods. 2 ZEÚ sa majú vykladať v tom zmysle, že vnútroštátna právna úprava, ktorá umožňuje štátnemu orgánu uložiť poskytovateľom elektronických komunikačných služieb povinnosť odovzdávať bezpečnostným a spravodajským službám údaje o prenose dát a polohe na účely ochrany národnej bezpečnosti, patrí do pôsobnosti tejto smernice.

O druhej otázke

50 Svojou druhou otázkou sa vnútroštátny súd v podstate pýta, či sa má článok 15 ods. 1 smernice 2002/58 v spojení s článkom 4 ods. 2 ZEÚ, ako aj s článkami 7, 8 a 11 a s článkom 52 ods. 1 Charty vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá umožňuje štátnemu orgánu na účely ochrany národnej bezpečnosti uložiť poskytovateľom elektronických komunikačných služieb povinnosť vyžadujúcu všeobecné a nediferencované odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám.

51 Na úvod treba pripomenúť, že podľa informácií uvedených v návrhu na začatie prejudiciálneho konania § 94 zákona z roku 1984 dovoľuje ministrovi uložiť poskytovateľom elektronických komunikačných služieb vo forme pokynu povinnosť, ak to považuje za potrebné v záujme národnej bezpečnosti alebo v záujme vzťahov s cudzou vládou, odovzdať bezpečnostným a spravodajským službám hromadné údaje o komunikáciách, pričom tieto údaje zahŕňajú údaje o prenose dát a polohe, ako aj informácie o použitých službách v zmysle § 21 ods. 4 a 6 RIPA. Toto posledné uvedené ustanovenie zahŕňa okrem iného údaje potrebné na identifikáciu zdroja komunikácie a jej adresáta, určenie dátumu, času, trvania a typu komunikácie, identifikácie použitého zariadenia a polohy koncových zariadení

a komunikácie, teda údaje, medzi ktoré patria najmä meno a adresa používateľa, telefónne čísla volajúceho a volaného, IP adresy zdroja a príjemcu komunikácie, ako aj adresy navštívených internetových stránok.

52 Takéto poskytovanie údajov prenosom sa týka všetkých používateľov elektronických komunikačných prostriedkov, pričom sa nespresňuje, či sa tento prenos musí uskutočniť v reálnom čase alebo až po určitom čase. Podľa informácií uvedených v návrhu na začatie prejudiciálneho konania sú tieto údaje po vykonaní prenosu uchovávané bezpečnostnými a spravodajskými službami a podobne ako iné databázy týchto služieb sú im k dispozícii na účely ich činností. Takto vyzbierané údaje, ktoré sú hromadne a automatizovane spracovávané a analyzované, môžu byť porovnané s inými databázami obsahujúcimi rôzne kategórie hromadných osobných údajov alebo sprístupnené mimo tieto služby a do tretích štátov. Napokon tieto operácie nepodliehajú predchádzajúcemu povoleniu súdu alebo nezávislého správneho orgánu a dotknuté osoby nie sú o nich nijako informované.

53 Účelom smernice 2002/58, ako vyplýva najmä z jej odôvodnení 6 a 7, je chrániť používateľov elektronických komunikačných služieb pred rizikami pre osobné údaje a súkromie, ktoré vyplývajú z nových technológií a predovšetkým zo zvyšovania kapacity automatického uchovávania a spracovávania údajov. Táto smernica, ako sa uvádza v jej odôvodnení 2, sa snaží najmä o plné zabezpečenie práv stanovených v článkoch 7 a 8 Charty. V tejto súvislosti z dôvodovej správy k návrhu smernice Európskeho parlamentu a Rady týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií [KOM(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“.

54 Článok 5 ods. 1 smernice 2002/58 na tieto účely stanovuje, že „členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí“. Toto isté ustanovenie tiež zdôrazňuje, že „[členské štáty] zakážu najmä počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami zo strany iných osôb než sú užívatelia bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1“, a spresňuje, že „tento odsek nebráni technickému uloženiu, ak je to potrebné s cieľom prenosu správy, bez vplyvu na princíp dôvernosti“.

55 Tento článok 5 ods. 1 teda zakotvuje zásadu dôvernosti elektronických komunikácií a príslušných údajov o prenose dát a zahŕňa okrem iného, že sa akýmkoľvek iným osobám než používateľom v zásade zakazuje bez súhlasu týchto používateľov uchovávať tieto komunikácie a tieto údaje. Toto ustanovenie sa vzhľadom na všeobecnú povahu jeho znenia nevyhnutne vzťahuje na všetky operácie, ktoré umožňujú tretím osobám oboznámiť sa s komunikáciou a s ňou súvisiacimi údajmi na iné účely ako na prenos správy.

56 Zákaz zachytávať komunikáciu a s tým súvisiace údaje uvedený v článku 5 ods. 1 smernice 2002/58 sa teda vzťahuje na akúkoľvek formu sprístupnenia údajov o prenose dát a polohe poskytovateľmi elektronických komunikačných služieb orgánom verejnej moci, akými sú bezpečnostné a spravodajské služby, ako aj uchovávanie uvedených údajov týmito orgánmi bez ohľadu na ich neskoršie využitie.

57 Prijatím tejto smernice tak normotvorca Únie konkretizoval práva zakotvené v článkoch 7 a 8 Charty, takže používatelia elektronických komunikačných prostriedkov majú v zásade právo očakávať, že ich komunikácia a s ňou súvisiace údaje zostanú v prípade chýbajúceho súhlasu z ich strany anonymizované a nebudú môcť byť predmetom zaznamenania (rozsudok zo 6, októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, bod 109).

58 Článok 15 ods. 1 smernice 2002/58 však umožňuje členským štátom zaviesť výnimky z povinnosti stanovenej v článku 5 ods. 1 uvedenej smernice, podľa ktorej sú tieto štáty povinné zabezpečiť dôvernosť osobných údajov, ako aj z príslušných povinností uvedených najmä v článkoch 6 a 9 uvedenej smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti, obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie elektronického komunikačného systému. Na tento účel môžu členské štáty okrem iného prijať legislatívne opatrenia, ktoré stanovujú uchovávanie údajov na obmedzené obdobie, ak je to odôvodnené niektorým z týchto dôvodov.

59 Za týchto okolností možnosť odchýliť sa od práv a povinností stanovených v článkoch 5, 6 a 9 smernice 2002/58 nemôže odôvodniť, že výnimka zo zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov, a najmä výnimka zo zákazu uchovávať tieto údaje výslovne uvedená v článku 5 tejto smernice, sa stane pravidlom (pozri v tomto zmysle rozsudky z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 89 a 104, ako aj zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, bod 111).

60 Z článku 15 ods. 1 tretej vety smernice 2002/58 okrem toho vyplýva, že členské štáty sú oprávnené prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článkoch 5, 6 a 9 tejto smernice len pri dodržaní všeobecných zásad práva Únie, vrátane zásady proporcionality, a základných práv zaručených Chartou. V tejto súvislosti Súdny dvor už rozhodol, že povinnosť uložená poskytovateľom elektronických komunikačných služieb zo strany členského štátu na základe vnútroštátnej právnej úpravy, 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 sa týkajú ochrany súkromia a ochrany osobných údajov, ale aj s článkom 11 Charty týkajúcim sa slobody prejavu (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, body 25 a 70, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 91 a 92, ako aj citovanú judikatúru).

61 Tie isté otázky vyvstávajú aj pri iných druhoch spracovania údajov, ako je ich odovzdávanie iným osobám ako používateľom alebo prístup k týmto údajom na účely ich využitia [pozri analogicky stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 122 a 123, ako aj citovanú judikatúru].

62 Pri výklade článku 15 ods. 1 smernice 2002/58 je preto potrebné prihliadať nielen na význam práva na rešpektovanie súkromného života zaručeného v článku 7 Charty a práva na ochranu osobných údajov zaručeného v jej článku 8, ako vyplýva z judikatúry Súdneho dvora, ale aj na dôležitosť práva na slobodu prejavu, pričom toto základné právo zaručené v článku 11 Charty predstavuje jednu zo základných podstát demokratickej a pluralitnej spoločnosti a je súčasťou hodnôt, na ktorých je Únia v súlade s článkom 2 ZEÚ založená (pozri v tomto zmysle rozsudky zo 6. marca 2001, Connolly/Komisia, C-274/99 P, EU:C:2001:127, bod 39, a z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 93 a citovanú judikatúru).

63 Práva zakotvené v článkoch 7, 8 a 11 Charty však nie sú absolútnymi výsadami, ale musia sa vnímať vo vzťahu k ich úlohe v spoločnosti (pozri v tomto zmysle rozsudok zo 16. júla 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 172, ako aj citovanú judikatúru).

64 Charta, ako vyplýva z jej článku 52 ods. 1, totiž pripúšťa obmedzenia výkonu týchto práv, pokiaľ sú tieto obmedzenia stanovené zákonom, rešpektujú podstatu uvedených práv a – za predpokladu dodržiavania zásady proporcionality – sú nevyhnutné, pričom skutočne zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo potrebe chrániť práva a slobody iných.

65 Treba ďalej uviesť, že požiadavka, podľa ktorej musí byť každé obmedzenie výkonu základných práv stanovené zákonom, predpokladá, že samotný právny základ, ktorý umožňuje zásah do týchto práv, musí vymedzovať rozsah obmedzenia výkonu dotknutého práva (rozsudok zo 16. júla 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 175 a citovaná judikatúra).

66 Pokiaľ ide o dodržiavanie zásady proporcionality, článok 15 ods. 1 prvá veta smernice 2002/58 stanovuje, že členské štáty môžu prijať opatrenie, ktoré predstavuje výnimku zo zásady dôvernosti komunikácie a príslušných údajov o prenose, ak ide o „nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti“, so zreteľom na ciele stanovené v tomto ustanovení. Odôvodnenie 11 tejto smernice spresňuje, že opatrenie tohto druhu musí byť „prísne“ proporcionálne vo vzťahu k zamýšľanému účelu.

67 V tejto súvislosti treba pripomenúť, že ochrana základného práva na rešpektovanie súkromného života v súlade s ustálenou judikatúrou Súdneho dvora vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je striktne nevyhnutné. Okrem toho nemožno sledovať cieľ všeobecného záujmu bez zohľadnenia skutočnosti, že musí byť zosúladený so základnými právami dotknutými opatrením, a to náležitým vyvážením cieľa všeobecného záujmu a dotknutých práv [pozri v tomto zmysle 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, body 76, 77 a 86, ako aj z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, bod 52; stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 140].

68 Na účely splnenia požiadavky proporcionality musí právna úprava stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých osobné údaje sú dotknuté, mali dostatočné záruky umožňujúce účinne chrániť tieto údaje pred rizikami zneužitia. Táto právna úprava musí byť podľa vnútroštátneho práva právne záväzná a musí najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracúvané automaticky, najmä ak existuje značné riziko neoprávneného prístupu k týmto údajom. Tieto úvahy platia najmä vtedy, keď ide o ochranu osobitnej kategórie osobných údajov, ktorú tvoria citlivé údaje [pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, body 54 a 55, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 117; stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 141].

69 Pokiaľ ide o otázku, či vnútroštátna právna úprava, o akú ide vo veci samej, spĺňa požiadavky článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, treba uviesť, že odovzdávanie údajov o prenose dát a polohe iným osobám než používateľom, ako sú napríklad bezpečnostné a spravodajské služby, predstavuje výnimku zo zásady dôvernosti. Ak sa táto operácia vykonáva, ako je tomu v prejednávanej veci, všeobecne a nediferencovane, má za následok, že z odchýlenia sa od základnej povinnosti zabezpečiť dôvernosť údajov sa stáva pravidlo, zatiaľ čo systém zavedený smernicou 2002/58 vyžaduje, aby takáto odchýlka zostala výnimkou.

70 Okrem toho v súlade s ustálenou judikatúrou Súdneho dvora predstavuje odovzdávanie údajov o prenose dát a polohe tretím osobám zásah do základných práv zakotvených v článkoch 7 a 8 Charty bez ohľadu na neskoršie využitie týchto údajov. V tejto súvislosti nie je dôležité, či predmetné informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu tohto zásahu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 124 a 126, ako aj citovanú judikatúru, a rozsudok zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, body 115 a 116].

71 Zásah do práva zakotveného v článku 7 Charty, ktorý spôsobuje odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám, treba považovať za obzvlášť závažný najmä vzhľadom na citlivú povahu informácií, ktoré môžu z týchto údajov vyplynúť, a najmä možnosť vytvoriť z nich profily dotknutých osôb, pričom takáto informácia je rovnako citlivá ako samotný obsah komunikácie. Navyše môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania (pozri analogicky rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, body 27 a 37, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 99 a 100).

72 Ďalej treba uviesť, že odovzdávanie údajov o prenose dát a polohe orgánom verejnej moci na bezpečnostné účely môže samo osebe zasahovať do práva na rešpektovanie komunikácie zakotveného v článku 7 Charty a odrádzať používateľov elektronických komunikačných prostriedkov od uplatňovania ich slobody prejavu zaručenej v článku 11 Charty. Tento odrádzajúci účinok môže mať vplyv najmä na osoby, ktorých komunikácia podľa vnútroštátnych pravidiel podlieha služobnému tajomstvu, a oznamovateľov, ktorých činnosti sú chránené smernicou Európskeho parlamentu a Rady (EÚ) 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie (Ú. v. EÚ L 305, s. 17). Okrem toho je tento účinok ešte závažnejší vzhľadom na veľké množstvo a rôznorodosť uchovávaných údajov (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, bod 28; z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 101, ako aj zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, bod 118).

73 Napokon vzhľadom na značné množstvo údajov o prenose dát a polohe, ktoré možno nepretržite uchovávať na základe opatrenia všeobecného uchovávania, a citlivú povahu informácií, ktoré sa dajú z týchto údajov získať, už samotné uchovávanie uvedených údajov poskytovateľmi elektronických komunikačných služieb v sebe zahŕňa riziká zneužitia a neoprávneného prístupu.

74 Pokiaľ ide o ciele, ktoré by mohli odôvodniť takéto zásahy, konkrétne cieľ ochrany národnej bezpečnosti dotknutý vo veci samej, treba na úvod uviesť, že článok 4 ods. 2 ZEÚ stanovuje, že národná bezpečnosť zostáva vo výlučnej zodpovednosti každého členského štátu. Táto zodpovednosť zodpovedá prvoradému záujmu chrániť základné funkcie štátu a základné záujmy spoločnosti a zahŕňa predchádzanie a potláčanie činností, ktoré môžu vážne destabilizovať základné politické, ústavné, hospodárske alebo sociálne štruktúry krajiny a najmä priamo ohroziť spoločnosť, obyvateľstvo alebo samotný štát, akými sú napríklad teroristické aktivity (rozsudok zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, bod 135).

75 Význam cieľa ochrany národnej bezpečnosti v spojení s článkom 4 ods. 2 ZEÚ tak presahuje význam ostatných cieľov uvedených v článku 15 ods. 1 smernice 2002/58, a to najmä cieľov boja proti trestnej činnosti vo všeobecnosti, hoci aj závažnej, a ochrany verejnej bezpečnosti. Také hrozby, akými sú hrozby uvedené v predchádzajúcom bode, sa totiž svojou povahou a osobitnou závažnosťou odlišujú od všeobecného či dokonca závažného rizika vzniku napätia alebo narušenia v oblasti verejnej bezpečnosti. Cieľ ochrany národnej bezpečnosti teda môže, pokiaľ sú splnené ostatné požiadavky stanovené v článku 52 ods. 1 Charty, odôvodniť opatrenia, ktoré zasahujú do základných práv závažnejšie než tie, ktoré by mohli byť odôvodnené týmito ostatnými cieľmi (rozsudok zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, bod 136).

76 Na to, aby vnútroštátna právna úprava zasahujúca do základných práv zakotvených v článkoch 7 a 8 Charty spĺňala požiadavku proporcionality pripomenutú v bodoch 67 tohto rozsudku, podľa ktorej výnimky a obmedzenia v súvislosti s ochranou osobných údajov nesmú pôsobiť nad rámec toho, čo je striktne nevyhnutné, musí dodržiavať požiadavky vyplývajúce z judikatúry uvedenej v bodoch 65, 67 a 68 tohto rozsudku.

77 Konkrétne v súvislosti s prístupom orgánu k osobným údajom sa právna úprava nemôže obmedziť len na požiadavku, aby prístup orgánov k údajom zodpovedal cieľu sledovanému touto právnou úpravou, ale musí takisto stanoviť hmotnoprávne a procesné podmienky upravujúce toto využívanie [pozri analogicky stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 192 a citovanú judikatúru].

78 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, vnútroštátna právna úprava prístupu k údajom o prenose dát a polohe sa musí zakladať na objektívnych kritériách s cieľom určiť okolnosti a podmienky, za akých sa má poskytnúť prístup príslušným vnútroštátnym orgánom k dotknutým údajom (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 119 a citovanú judikatúru).

79 Tieto požiadavky sa *a fortiori* uplatňujú na také legislatívne opatrenie, o aké ide vo veci samej, na základe ktorého môže príslušný vnútroštátny orgán uložiť poskytovateľom elektronických komunikačných služieb povinnosť všeobecne a nediferencovane sprístupniť údaje o prenose dát a polohe prenosom bezpečnostným a spravodajským službám. V dôsledku takéhoto prenosu sú totiž tieto údaje sprístupnené orgánom verejnej moci [pozri analogicky stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 212].

80 Keďže odovzdávanie údajov o prenose dát a polohe sa uskutočňuje všeobecne a nediferencovane, týka sa globálne všetkých osôb používajúcich elektronické komunikačné služby. Uplatňuje sa teda aj na osoby, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť s cieľom ochrany národnej bezpečnosti, a najmä bez toho, aby bola preukázaná súvislosť medzi údajmi, ktorých odovzdanie sa umožňuje, a hrozbou pre národnú bezpečnosť (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights Ireland a i., C-293/12 a C-594/12, EU:C:2014:238, body 57 a 58, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 105). Vzhľadom na skutočnosť, že odovzdávanie takýchto údajov orgánom verejnej moci zodpovedá – v súlade s konštatovaním uvedeným v bode 79 tohto rozsudku – ich sprístupneniu, treba dospieť k záveru, že právna úprava umožňujúca všeobecné a nediferencované odovzdávanie údajov orgánom verejnej moci zahŕňa všeobecný prístup.

81 Z toho vyplýva, že vnútroštátna právna úprava, ktorá poskytovateľom elektronických komunikačných služieb ukladá povinnosť všeobecne a nediferencovane poskytovať údaje o prenose dát a polohe prenosom bezpečnostným a spravodajským službám, 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 článkom 4 ods. 2 ZEÚ, ako aj s článkami 7, 8 a 11 a s článkom 52 ods. 1 Charty.

82 Vzhľadom na všetky predchádzajúce úvahy treba na druhú otázku odpovedať tak, že článok 15 ods. 1 smernice 2002/58 v spojení s článkom 4 ods. 2 ZEÚ, ako aj s článkami 7, 8 a 11 a s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá umožňuje štátnemu orgánu uložiť poskytovateľom elektronických komunikačných služieb povinnosť vyžadujúcu všeobecné a nediferencované odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám na účely ochrany národnej bezpečnosti.

O trovách

83 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 vnútroštátnym súdom, o trovách konania rozhodne tento vnútroštátny súd. 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 1 ods. 3, článok 3 a článok 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, v spojení s článkom 4 ods. 2 ZEÚ sa majú vykladať v tom zmysle, že vnútroštátna právna úprava, ktorá umožňuje štátnemu orgánu uložiť poskytovateľom elektronických komunikačných služieb povinnosť odovzdávať bezpečnostným a spravodajským službám údaje o prenose dát a polohe na účely ochrany národnej bezpečnosti, patrí do pôsobnosti tejto smernice.**

2. **Článok 15 ods. 1 smernice 2002/58, zmenenej smernicou 2009/136, v spojení s článkom 4 ods. 2 ZEÚ, ako aj s článkami 7, 8 a 11 a s článkom 52 ods. 1 Charty základných práv Európskej únie sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá umožňuje štátnemu orgánu na účely ochrany národnej bezpečnosti uložiť poskytovateľom elektronických komunikačných služieb povinnosť vyžadujúcu všeobecné a nediferencované odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám.**

Podpisy