Sbírka soudních rozhodnutí

ROZSUDEK SOUDNÍHO DVORA (velkého senátu)

6. října 2020*

„Řízení o předběžné otázce – Zpracování osobních údajů v odvětví elektronických komunikací – Poskytovatelé služeb elektronických komunikací – Plošné a nerozlišující předávání provozních a lokalizačních údajů – Zajištění národní bezpečnosti – Směrnice 2002/58/ES – Oblast působnosti – Článek 1 odst. 3 a článek 3 – Důvěrný charakter elektronických sdělení – Ochrana – Článek 5 a čl. 15 odst. 1 – Listina základních práv Evropské unie – Články 7, 8 a 11 a čl. 52 odst. 1 – Článek 4 odst. 2 SEU“

Ve věci C-623/17,

jejímž předmětem je žádost o rozhodnutí o předběžné otázce na základě článku 267 SFEU, podaná rozhodnutím Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království) ze dne 18. října 2017, došlým Soudnímu dvoru dne 31. října 2017, v řízení

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,

SOUDNÍ DVŮR (velký senát),

ve složení K. Lenaerts, předseda, R. Silva de Lapuerta, místopředsedkyně, J.-C. Bonichot, A. Arabadžev, A. Prechal, M. Safjan, P. G. Xuereb a L. S. Rossi, předsedové senátů, J. Malenovský, L. Bay Larsen, T. von Danwitz (zpravodaj), C. Toader, K. Jürimäe, C. Lycourgos a N. Piçarra, soudci,

generální advokát: M. Campos Sánchez-Bordona,

vedoucí soudní kanceláře: C. Strömholm, radová,

s přihlédnutím k písemné části řízení a po jednáních konaných ve dnech 9. a 10. září 2019,

* Jednací jazyk: angličtina.

s ohledem na vyjádření předložená:

– za Privacy International B. Jaffeym a T. de la Mare, QC, D. Cashmanem, solicitor, jakož i H. Royem, avocat,

– za vládu Spojeného království Z. Lavery, D. Guðmundsdóttir a S. Brandonem, jako zmocněnci, ve spolupráci s G. Facennou a D. Beardem, QC, jakož i s C. Knightem a R. Palmerem, barristers,

– za belgickou vládu P. Cottinem a J.-C. Halleuxem, jako zmocněnci, ve spolupráci s J. Vanpraetem, advocaat, a E. de Lophem, avocat,

– za českou vládu M. Smolkem, J. Vláčilem a O. Serdulou, jako zmocněnci,

– za německou vládu původně M. Hellmannem, R. Kanitzem, D. Klebsem a T. Henzem, poté J. Möllerem, M. Hellmannem, R. Kanitzem a D. Klebsem, jako zmocněnci,

– za estonskou vládu A. Kalbus, jako zmocněnkyní,

– za irskou vládu M. Browne, G. Hodge a A. Joycem, jako zmocněnci, ve spolupráci s D. Fennellym, barrister,

– za španělskou vládu původně L. Aguilera Ruizem a M. J. García-Valdecasas Dorrego, poté L. Aguilera Ruizem, jako zmocněnci,

– za francouzskou vládu původně E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrunem, D. Colasem a D. Duboisem, poté E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrunem a D. Duboisem, jako zmocněnci,

– za kyperskou vládu E. Symeonidou a E. Neofytou, jako zmocněnkyněmi,

– za lotyšskou vládu původně V. Soņeca a I. Kucina, poté V. Soņeca, jako zmocněnkyněmi,

– za maďarskou vládu původně G. Koósem, M. Z. Fehérem, G. Tornyaim a Z. Wagner, poté G. Koósem a M. Z. Fehérem, jako zmocněnci,

– za nizozemskou vládu C. S. Schillemans a M. K. Bulterman, jako zmocněnkyněmi,

– za polskou vládu B. Majczynou, J. Sawickou a M. Pawlickou, jako zmocněnci,

– za portugalskou vládu L Inez Fernandesem, M. Figueiredem a F. Aragão Homem, jako zmocněnci,

– za švédskou vládu původně A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren a A. Alriksson, poté H. Shev, C. Meyer-Seitz, L. Zettergren a A. Alriksson, jako zmocněnkyněmi,

– za norskou vládu T. B. Lemingem, M. Emberlandem a J. Vangsnesem, jako zmocněnci,

– za Evropskou komisi původně H. Kranenborgem, M. Wasmeierem, D. Nardim a P. Costa de Oliveira, poté H. Kranenborgem, M. Wasmeierem a D. Nardim, jako zmocněnci,

– za Evropského inspektora ochrany údajů T. Zerdickem a A. Buchta, jako zmocněnci,

po vyslechnutí stanoviska generálního advokáta na jednání konaném dne 15. ledna 2020,

vydává tento

Rozsudek

1 Žádost o rozhodnutí o předběžné otázce se týká výkladu čl. 1 odst. 3 a čl. 15 odst. 1 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. 2002, L 201, s. 37; Zvl. vyd. 13/29, s. 514, oprava Úř. věst. 2014, L 290, s. 11), ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009 (Úř. věst. 2009, L 337, s. 11) (dále jen „směrnice 2002/58“), ve spojení s čl. 4 odst. 2 SEU, jakož i s články 7 a 8 a čl. 52 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“).

2 Tato žádost byla předložena v rámci sporu mezi Privacy International na straně jedné a Secretary of State for Foreign and Commonwealth Affairs (ministr zahraničních věcí a věcí Společenství národů, Spojené království), Secretary of State for the Home Departement (ministr vnitra, Spojené království), Government Communications Headquarters (vládní komunikační ústředí, Spojené království) (dále jen „GCHQ“), Security Service (bezpečnostní služba, Spojené království, dále jen „MI5“) a Secret Intelligence Service (tajná zpravodajská služba, Spojené království, dále jen „MI6“) na straně druhé, jehož předmětem je legalita právní úpravy, která bezpečnostním a zpravodajským službám umožňuje shromažďovat a využívat hromadné komunikační údaje *(bulk communications data)*.

Právní rámec

Unijní právo

Směrnice 95/46

3 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. 1995, L 281, s. 31; Zvl. vyd. 13/15, s. 355) byla s účinkem od 25. května 2018 zrušena nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Úř. věst. 2016, L 119, s. 1; oprava Úř. věst. 2018, L 127, s. 2). Článek 3 uvedené směrnice, nadepsaný „Oblast působnosti“, zněl:

„1. Tato směrnice se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů, jakož i na neautomatizované zpracování osobních údajů, které jsou obsaženy v rejstříku nebo do něj mají být zařazeny.

2. Tato směrnice se nevztahuje na zpracování osobních údajů:

– prováděné pro výkon činností, které nespadají do oblasti působnosti práva Společenství a jsou uvedeny [které nespadají do oblasti působnosti práva Společenství, jako jsou činnosti uvedené] v hlavě V a VI [SEU], a v každém případě na zpracování, které se týká veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské stability státu, pokud jsou tato zpracování spojená s otázkami bezpečnosti státu) a činnosti státu v oblasti trestního práva,

– prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností.“

Směrnice 2002/58

4 V bodech 2, 6, 7, 11, 22, 26 a 30 odůvodnění směrnice 2002/58 se uvádí:

„(2) tato směrnice usiluje o respektování základních práv a zachovává zásady uznané zejména v [Listině]. Tato směrnice zejména usiluje o to, aby byla plně dodržována práva stanovená v článcích 7 a 8 uvedené listiny;

[…]

(6) internet převrací tradiční struktury trhu tím, že poskytuje společnou, obecnou infrastrukturu pro široký okruh služeb elektronických komunikací. Veřejně dostupné služby elektronických komunikací prostřednictvím internetu otevírají uživatelům nové možnosti, ale zároveň vytvářejí i nová rizika pro jejich osobní údaje a soukromí;

(7) v případě sítí veřejných komunikací je nutno přijmout zvláštní právní, regulační a technická ustanovení na ochranu základních práv a svobod fyzických osob a ochranu oprávněných zájmů právnických osob, zejména s ohledem na zvyšující se kapacitu automatického uchovávání a zpracování údajů týkajících se účastníků a uživatelů.

[…]

(11) tato směrnice, obdobně jako směrnice [95/46], se netýká ochrany základních práv a svobod ve vztahu k činnostem, které se neřídí právem [Unie]. Proto tato směrnice nemění stávající rovnováhu mezi právem jednotlivce na soukromí a možností, aby členské státy přijaly opatření uvedená v čl. 15 odst. 1 této směrnice, která jsou nezbytná pro ochranu veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a pro prosazování trestního práva. Tato směrnice se tedy nedotýká možnosti členských států provádět zákonné zachycování elektronických sdělení nebo přijímat jiná opatření, je-li to nezbytné pro některý z těchto účelů a je-li to v souladu s [e]vropskou [Ú]mluvou o ochraně lidských práv a základních svobod [podepsanou v Římě dne 4. listopadu 1950], jak je vykládána v rozhodnutích Evropského soudu pro lidská práva. Tato opatření musí být vhodná, plně přiměřená vzhledem k zamýšlenému účelu a nezbytná v demokratické společnosti a musí být předmětem odpovídajících záruk v souladu s [e]vropskou [Ú]mluvou o ochraně lidských práv a základních svobod;

[…]

(22) zákaz uchovávat sdělení a s nimi spojené provozní údaje jinými osobami než samotnými uživateli nebo bez jejich souhlasu neznamená zákaz jakéhokoli automatického, zprostředkovaného a přechodného uchovávání takových informací, pokud k němu dochází výlučně z důvodu provedení přenosu v síti elektronických komunikací a za předpokladu, že informace nejsou uchovávány po dobu delší než nezbytně nutnou pro účely přenosu a řízení provozu, a že po dobu tohoto uchovávání zůstane zajištěna důvěrnost. Je-li to nezbytné pro zefektivnění dalšího přenosu jakýchkoli veřejně dostupných informací jiným příjemcům služby na základě jejich žádosti, neměla by tato směrnice bránit dalšímu uchovávání takových informací za předpokladu, že tyto informace budou kdykoli bez omezení dostupné veřejnosti a že jakékoli údaje o jednotlivých účastnících či uživatelích, kteří tyto informace požadují, budou vymazány;

[…]

(26) údaje o účastnících, které jsou zpracovávány v rámci sítí elektronických komunikací pro navázání spojení a přenos informací, obsahují informace o soukromém životě fyzických osob a dotýkají se práva na ochranu jejich korespondence nebo se dotýkají oprávněných zájmů právnických osob.

Takové údaje je možno uchovávat pouze v rozsahu, který je nezbytný pro poskytování služby pro účely účtování a platby za propojení, a to po omezenou dobu. Jakékoli další zpracování takových údajů […] je přípustné pouze za předpokladu, že účastník s tímto souhlasil na základě přesných a úplných informací o druhu následného zamýšleného zpracování, které obdržel od poskytovatele veřejně dostupných služeb elektronických komunikací, spolu s informací o právu účastníka nedat takový souhlas nebo svůj souhlas k takovému zpracování vzít zpět. Provozní údaje používané pro marketing komunikačních služeb nebo pro poskytování služeb s přidanou hodnotou by měly být po poskytnutí služby vymazány nebo anonymizovány. […]

[…]

(30) systémy pro zajišťování sítí a služeb elektronických komunikací musí být navrženy tak, aby omezily na nutné minimum množství nezbytných osobních údajů. […]“

5 Článek 1 směrnice 2002/58, nadepsaný „Oblast působnosti a cíl“, stanoví:

„1. Touto směrnicí se harmonizují předpisy členských států požadované pro zajištění rovnocenné úrovně ochrany základních práv a svobod, zejména práva na soukromí a zachování důvěrnosti informací, se zřetelem na zpracování osobních údajů v odvětví elektronických komunikací, a pro zajištění volného pohybu těchto údajů a elektronických komunikačních zařízení a služeb v[Evropské unii].

2. Ustanovení této směrnice upřesňují a doplňují směrnici [95/46] pro účely uvedené v odstavci 1. Navíc poskytují ochranu oprávněných zájmů účastníků, kteří jsou právnickými osobami.

3. Tato směrnice se nevztahuje na činnosti, které nespadají do oblasti působnosti Smlouvy o [FEU], jako činnosti uvedené v hlavách V a VI Smlouvy o Evropské unii, a v žádném případě na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a na činnosti státu v oblasti trestního práva.“

6 Článek 2 této směrnice, nadepsaný „Definice“, stanoví:

„Není-li stanoveno jinak, použijí se definice uvedené ve směrnici [95/46] a směrnici Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice) [(Úř. věst. 2002, L 108, s. 33; Zvl. vyd. 13/29, s. 349)].

Použijí se rovněž tyto definice:

(a) ‚uživatelem‘ se rozumí jakákoli fyzická osoba používající veřejně dostupnou službu elektronické komunikace pro soukromé či obchodní účely, přičemž není nezbytně nutné, aby byla účastníkem této služby;

(b) ‚provozními údaji‘ se rozumějí jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování;

(c) ‚lokalizačními údaji‘ se rozumějí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací;

(d) ‚sdělením' se rozumí jakákoli informace, která se vyměňuje nebo přenáší mezi určitým počtem zúčastněných stran prostřednictvím veřejně dostupné služby elektronických komunikací; toto nezahrnuje informace přenášené jako součást vysílání pro veřejnost prostřednictvím sítě elektronických komunikací s výjimkou případů, kdy lze informace přiřadit k identifikovatelnému účastníku nebo uživateli, který tyto informace přijímá;

[…]"

7 Článek 3 uvedené směrnice, nadepsaný „Dotčené služby", stanoví:

„Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v[Unii], včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů."

8 Článek 5 směrnice 2002/58, nadepsaný „Důvěrný charakter sdělení", stanoví:

„1. Členské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1. Tento odstavec nebrání technickému uchovávání, které je nezbytné pro přenos sdělení, aniž by tím byla dotčena zásada důvěrnosti.

[…]

3. Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí [95/46], mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal."

9 Článek 6 směrnice 2002/58, nadepsaný „Provozní údaje", stanoví:

„1. Provozní údaje vztahující se k účastníkům a uživatelům zpracovávané a uchovávané provozovatelem veřejné komunikační sítě nebo poskytovatelem veřejně dostupné služby elektronických komunikací, musí být vymazány nebo anonymizovány, jakmile již nejsou potřebné pro přenos sdělení, aniž by tímto byly dotčeny odstavce 2, 3 a 5 tohoto článku a čl. 15 odst. 1.

2. Je možno zpracovávat provozní údaje nezbytné pro účely účtování a stanovení plateb za propojení. Takovéto zpracování je přípustné pouze do konce období, v němž lze právně napadnout účet či uplatňovat nárok na platbu.

3. Pro potřeby marketingu služeb elektronických komunikací nebo pro poskytování služeb s přidanou hodnotou může poskytovatel veřejně dostupných služeb elektronických komunikací zpracovávat údaje uvedené v odstavci 1 pouze v rozsahu nezbytném a po dobu nezbytnou pro tyto služby nebo marketing, pokud k tomu dal předem souhlas účastník nebo uživatel, jehož se údaje týkají. Účastníci či uživatelé musí mít možnost kdykoliv svůj souhlas se zpracováním provozních údajů vzít zpět.

[…]

5. Zpracování provozních údajů podle odstavců 1, 2, 3 a 4 musí být omezeno na osoby, které jednají z pověření provozovatelů veřejných komunikačních sítí a poskytovatelů veřejně dostupných služeb elektronických komunikací, a které se zabývají účtováním nebo řízením provozu, požadavky zákazníků, odhalováním podvodů, marketingem služeb elektronických komunikací nebo poskytováním služeb s přidanou hodnotou, a musí být omezeno na rozsah, který je nezbytný pro účely těchto činností.“

10 Článek 9 této směrnice, nadepsaný „Lokalizační údaje odlišné od provozních údajů“, v odstavci 1 stanoví:

„Mohou-li být zpracovávány lokalizační údaje odlišné od provozních údajů, které se vztahují k uživatelům nebo účastníkům veřejných komunikačních sítí nebo veřejně dostupných služeb elektronických komunikací, je možné tyto údaje zpracovávat pouze poté, co byly anonymizovány údaje, anebo se souhlasem uživatelů nebo účastníků v nezbytném rozsahu a po nezbytnou dobu pro poskytování služeb s přidanou hodnotou. Poskytovatel služeb musí informovat uživatele nebo účastníky před obdržením jejich souhlasu o druhu lokalizačních údajů odlišných od provozních údajů, které budou zpracovávány, o účelu a délce doby zpracování a o tom, zda budou údaje předány třetí osobě za účelem poskytování služeb s přidanou hodnotou. […]“

11 Článek 15 uvedené směrnice, nadepsaný „Použití některých ustanovení směrnice [95/46]“, v odstavci 1 stanoví:

„Členské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice [95/46]. Za tímto účelem mohou členské státy mimo jiné přijmout legislativní opatření umožňující uchovávání údajů po omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva [Unie], včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o Evropské unii.“

Nařízení 2016/679

12 Článek 2 nařízení 2016/679 stanoví:

„1. Toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

2. Toto nařízení se nevztahuje na zpracování osobních údajů prováděné:

a) při výkonu činností, které nespadají do oblasti působnosti práva Unie;

b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU;

[…]

d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

[…]“

13 Článek 4 tohoto nařízení stanoví:

„Pro účely tohoto nařízení se rozumí:

[…]

2) ‚zpracováním' jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

[…]"

14 Článek 23 odst. 1 téhož nařízení stanoví:

„Právo Unie nebo členského státu, které se na správce nebo zpracovatele vztahuje, může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v článcích 12 až 22 a v článku 34, jakož i v článku 5, v rozsahu, v jakém ustanovení tohoto článku odpovídají právům a povinnostem stanoveným v článcích 12 až 22, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit:

a) národní bezpečnost;

b) obranu;

c) veřejnou bezpečnost;

d) prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

e) jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu, včetně peněžních [měnových], rozpočtových a daňových záležitostí, veřejného zdraví a sociálního zabezpečení;

f) ochranu nezávislosti soudnictví a soudních řízení;

g) prevenci, vyšetřování, odhalování a stíhání porušování etických pravidel regulovaných povolání;

h) monitorovací, inspekční nebo regulační funkci spojenou, i pouze příležitostně, s výkonem veřejné moci v případech uvedených v písmenech a) až e) a g);

i) ochrany subjektu údajů nebo práv a svobod druhých;

j) vymáhání občanskoprávních nároků."

15 Článek 94 odst. 2 nařízení 2016/679 zní:

„Odkazy na zrušenou směrnici se považují za odkazy na toto nařízení. Odkazy na pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízenou článkem 29 směrnice [95/46] se považují za odkazy na Evropský sbor pro ochranu osobních údajů zřízený tímto nařízením."

Právo Spojeného království

16 Článek 94 Telecommunications Act 1984, ve znění účinném v době rozhodné z hlediska skutkového stavu (dále jen „zákon z roku 1984“), nadepsaný „Pokyny v zájmu národní bezpečnosti atd.“, stanoví:

„(1) Ministr může po konzultaci s osobou, na kterou se vztahuje tento článek, udělit této osobě obecné pokyny, které ministr považuje za nezbytné v zájmu národní bezpečnosti nebo v zájmu vztahů s vládou určité země nebo území mimo Spojené království.

(2) Považuje-li ministr za nezbytné postupovat tímto způsobem v zájmu národní bezpečnosti nebo v zájmu vztahů s vládou určité země nebo území mimo Spojené království, může po konzultaci s osobou, na kterou se vztahuje tento článek, udělit této osobě pokyn, kterým ji vyzve, aby (v závislosti na okolnostech daného případu) provedla nebo neprovedla určitý úkon specifikovaný v pokynu.

(2A) Ministr může vydat pokyn podle odstavce 1 nebo 2 jen tehdy, když má za to, že jednání vyžadované pokynem je přiměřené cíli, kterého má být tímto jednáním dosaženo.

(3) Osoba, na kterou se vztahuje tento článek, musí vykonat každý pokyn udělený jí ministrem podle tohoto článku, a to bez ohledu na jakoukoli jinou povinnost, která pro ni vyplývá z části 1 nebo části 2 kapitoly 1 Communications Act 2003 [zákon o komunikacích z roku 2003], a v případě pokynu uděleného provozovateli veřejné sítě elektronických komunikací i tehdy, když se daný pokyn vztahuje na tohoto provozovatele v postavení jiném než v postavení provozovatele takové sítě.

(4) Ministr uloží u každé z komor Parlamentu kopii každého pokynu vydaného na základě tohoto článku, ledaže by zpřístupnění daného pokynu bylo podle jeho názoru v rozporu se zájmy národní bezpečnosti nebo se zájmy vztahů s vládou určité země nebo území mimo Spojené království nebo s obchodními zájmy kohokoliv.

(5) Nikdo nesmí sdělit ani být na základě zákona či jinak nucen sdělit žádné informace týkající se opatření přijatých na základě tohoto článku, jestliže mu ministr oznámil, že podle názoru ministra je zpřístupnění těchto informací v rozporu se zájmy národní bezpečnosti nebo se zájmy vztahů s vládou určité země nebo území mimo Spojené království nebo s obchodními zájmy jiné osoby.

[…]

(8) Tento článek se vztahuje na [Office of communications (OFCOM)] a na poskytovatele veřejných sítí elektronických komunikací.“

17 Článek 21 odst. 4 a 6 Regulation of Investigatory Powers Act 2000 (zákon o úpravě vyšetřovacích pravomocí z roku 2010, dále jen „RIPA“) stanoví:

„(4) Pro účely této kapitoly se pojmem ‚komunikační údaje‘ rozumí:

a) jakékoli provozní údaje, jež jsou součástí sdělení nebo jsou k němu připojeny (odesílatelem nebo jinou osobou) pro účely jakékoli poštovní služby nebo telekomunikačního systému, jejichž prostřednictvím je nebo může být sdělení přenášeno,

b) jakékoli informace, jejichž součástí není žádný obsah sdělení [kromě informací spadajících pod písmeno a)] a které se týkají využití jakoukoli osobou
   (i) jakékoli poštovní nebo telekomunikační služby nebo
   (ii) jakékoli součásti telekomunikačního systému v souvislosti s poskytnutím jakékoli telekomunikační služby jakékoli osobě nebo použitím takové služby jakoukoli osobou,

c) jakékoli informace, které nespadají pod písmeno a) ani pod písmeno b) a které jsou v držení jakékoli osoby poskytující poštovní nebo telekomunikační službu nebo jsou takovou osobou získány, a to ve vztahu k osobám, kterým takovou službu poskytuje.

[…]

(6) Pro účely tohoto článku se pojmem ‚provozní údaje' ve vztahu k jakémukoli sdělení rozumí:

a) jakýkoli údaj identifikující nebo způsobilý identifikovat jakoukoli osobu, přístroj nebo polohu, které jsou zdrojem nebo adresátem přenášeného nebo potenciálně přenášeného sdělení;

b) jakýkoli údaj identifikující či vybírající nebo způsobilý identifikovat či vybrat zařízení, kterým je či může být přenášeno sdělení;

c) jakýkoli údaj obsahující signály pro zprovoznění přístroje používaného v komunikačním systému pro účely předání jakéhokoli sdělení nebo jeho části; a

d) jakýkoli údaj identifikující údaje, jež jsou součástí konkrétního sdělení nebo jsou k němu připojeny, či jiné údaje jako údaje, jež jsou součástí konkrétního sdělení nebo jsou k němu připojeny,

[…]"

18 Články 65 až 69 RIPA stanoví pravidla týkající se činnosti a pravomocí Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království). Je-li důvod se domnívat, že dochází k protiprávnímu shromažďování údajů, může být podle článku 65 tohoto zákona podána stížnost k tomuto soudu.

Spor v původním řízení a předběžné otázky

19 Začátkem roku 2015 vyšly veřejně najevo, zejména ve zprávě Intelligence and Security Committee of Parliament (výbor pro bezpečnost a zpravodajskou činnost Parlamentu, Spojené království), praktiky shromažďování a využívání hromadných komunikačních údajů různými bezpečnostními a zpravodajskými službami Spojeného království, konkrétně GCHQ, MI5 a MI6. Dne 5. června 2015 podala nevládní organizace Privacy International k Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království) proti ministrovi zahraničních věcí a věcí Společenství národů, ministrovi vnitra, jakož i těmto bezpečnostním a zpravodajským službám žalobu, kterou zpochybňuje legalitu těchto praktik.

20 Předkládající soud přezkoumal legalitu uvedených praktik nejprve vzhledem k vnitrostátnímu právu a k ustanovením evropské Úmluvy o ochraně lidských práv a základních svobod, podepsané v Římě dne 4. listopadu 1950 (dále jen „EÚLP"), a poté vzhledem k unijnímu právu. V rozsudku ze dne 17. října 2016 tento soud konstatoval, že žalovaní ve věci v původním řízení uznali, že bezpečnostní a zpravodajské služby v rámci svých činností shromažďovaly a využívaly soubory údajů o jednotlivcích spadající do různých kategorií *(bulk personal data)*, jako například biografické údaje, údaje o cestování, informace finanční či obchodní povahy, komunikační údaje, které mohou zahrnovat citlivé údaje spadající pod profesní tajemství, nebo též podklady pro žurnalistickou práci. Tyto údaje – získané různými způsoby, a to i utajeně – jsou analyzovány jejich propojením a automatizovaným zpracováním a mohou být zpřístupněny jiným osobám a orgánům a sdíleny se zahraničními partnery. V této souvislosti využívají bezpečnostní a zpravodajské služby i hromadné komunikační údaje shromážděné od poskytovatelů veřejných sítí elektronických komunikací zejména na základě pokynů ministra přijatých na základě článku 94 zákona z roku 1984. GCHQ tak činila od roku 2001 a MI5 od roku 2005.

21 Uvedený soud dospěl k závěru, že toto shromažďování a využívání údajů bylo v souladu s vnitrostátním právem a od roku 2015 – s výhradou dosud neposuzovaných otázek souvisejících s přiměřeností těchto praktik a s předáváním údajů třetím stranám – s článkem 8 EÚLP. K posledně zmíněnému aspektu uvedl, že mu byly předloženy důkazy týkající se příslušných záruk, zejména procesů přístupu a zpřístupňování mimo bezpečnostní a zpravodajské služby, podmínek ukládání údajů a existence nezávislých kontrol.

22 V souvislosti s legalitou shromažďování a využívání dotčených ve věci v původním řízení vzhledem k unijnímu právu se předkládající soud v rozsudku ze dne 8. září 2017 zabýval otázkou, zda uvedené praktiky vůbec spadají do oblasti působnosti unijního práva, a pokud ano, zda jsou s ním v souladu. V souvislosti s hromadnými komunikačními údaji tento soud shledal, že na základě článku 94 zákona z roku 1984 měli poskytovatelé sítí elektronických komunikací v případě, kdy ministr vydal pokyny v příslušném smyslu, povinnost poskytnout bezpečnostním a zpravodajským službám údaje shromážděné v rámci své ekonomické činnosti, na kterou se vztahuje unijní právo. To ovšem neplatilo pro shromažďování jiných údajů získávaných uvedenými službami bez využití takových donucovacích pravomocí. Na základě tohoto konstatování považoval tento soud za nezbytné požádat Soudní dvůr, aby určil, zda se na takový režim, jako je režim vyplývající z citovaného článku 94, vztahuje unijní právo, a pokud ano, zda a jak se na tento režim uplatní požadavky stanovené judikaturou vycházející z rozsudku ze dne 21. prosince 2016, Tele2 Sverige a Watson a další (C-203/15 a C-698/15, dále jen „rozsudek Tele2“, EU:C:2016:970).

23 V této souvislosti předkládající soud v žádosti o rozhodnutí o předběžné otázce uvádí, že podle uvedeného článku 94 může ministr udělovat poskytovatelům služeb elektronických komunikací obecné nebo konkrétní pokyny, které považuje za nezbytné v zájmu národní bezpečnosti nebo v zájmu vztahů s cizí vládou. S odkazem na definice obsažené v čl. 21 odst. 4 a 6 RIPA tento soud upřesňuje, že dotčené údaje zahrnují provozní údaje a informace o použitých službách ve smyslu posledně uvedeného ustanovení s tím, že vyloučen je jen obsah sdělení. Z těchto údajů a informací lze zejména zjistit, „kdo, kdy, kde a jak“ komunikoval. Tyto údaje jsou předávány bezpečnostním a zpravodajským službám, které je ukládají pro účely své činnosti.

24 Podle uvedeného soudu se režim dotčený ve věci v původním řízení liší od režimu, jenž zavedl Data Retention and Investigatory Powers Act 2014 (zákon o uchovávání údajů a vyšetřovacích pravomocech z roku 2014) dotčený ve věci, ve které byl vydán rozsudek ze dne 21. prosince 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970), protože tento posledně zmíněný režim předpokládal uchovávání údajů poskytovateli služeb elektronických komunikací a zpřístupnění těchto údajů nejen bezpečnostním a zpravodajským službám v zájmu národní bezpečnosti, ale i dalším orgánům veřejné moci podle jejich potřeb. Zmíněný rozsudek se navíc týkal trestního vyšetřování, a nikoli národní bezpečnosti.

25 Předkládající soud dodává, že databáze vytvářené bezpečnostními a zpravodajskými službami jsou předmětem nespecifického hromadného a automatizovaného zpracování, jehož účelem je odhalit případné neznámé hrozby. K tomu předkládající soud uvádí, že veškerá takto vytvořená metadata by měla být co nejkompletnější, aby mohla být k dispozici ona „kupka sena“, ve které je třeba najít „jehlu“, jež se v ní skrývá. V souvislosti s užitečností hromadného shromažďování údajů těmito službami a s metodami vyhledávání těchto údajů odkazuje uvedený soud konkrétně na závěry zprávy vypracované dne 19. srpna 2016 Davidem Andersonem, QC, v té době United Kingdom Independent Reviewer of Terrorism Legislation (nezávislý kontrolor právních předpisů Spojeného království o boji s terorismem), jenž při vypracovávání této zprávy vycházel z analýzy provedené týmem odborníků na zpravodajství a z výpovědí příslušníků bezpečnostních a zpravodajských služeb.

26 Předkládající soud také upřesňuje, že podle Privacy International je režim dotčený ve věci v původním řízení v rozporu s unijním právem, kdežto žalovaní ve věci v původním řízení se domnívají, že povinnost předávat údaje stanovená tímto režimem, přístup k těmto údajům ani jejich využití nespadají do pravomocí Unie, jak stanoví zejména čl. 4 odst. 2 SEU, podle kterého národní bezpečnost zůstává výhradní odpovědností každého členského státu.

27 V této souvislosti má předkládající soud na základě rozsudku ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346, body 56 a 59), týkajícího se předávání údajů jmenné evidence cestujících *(Passenger Name Record – PNR)* za účelem ochrany veřejné bezpečnosti, za to, že činnosti, které obchodní společnosti vyvíjejí v rámci zpracovávání a předávání údajů s cílem chránit národní bezpečnost, podle všeho nespadají do oblasti působnosti unijního práva. Podle jeho názoru se není třeba zabývat otázkou, zda dotčená činnost představuje zpracování údajů, ale jen otázkou, zda předmětem takové činnosti je ve své podstatě a svými účinky poskytovat podporu některé ze základních funkcí státu ve smyslu čl. 4 odst. 2 SEU prostřednictvím rámce stanoveného orgány veřejné moci v oblasti veřejné bezpečnosti.

28 Kdyby se na praktiky dotčené ve věci v původním řízení unijní právo přece jen vztahovalo, jsou podle předkládajícího soudu požadavky uvedené v bodech 119 až 125 rozsudku ze dne 21. prosince 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970), v kontextu národní bezpečnosti nepřiměřené a mohou oslabit možnosti bezpečnostních a zpravodajských služeb zvládat některé hrozby pro národní bezpečnost.

29 Za těchto okolností se Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí) rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

„V případě, že:

a) možnosti [bezpečnostních a zpravodajských služeb] využívat [hromadné komunikační údaje], které jsou jim dodány, jsou nezbytné pro ochranu národní bezpečnosti Spojeného království, včetně oblastí boje proti terorismu, kontrašpionáže a boje proti šíření jaderných zbraní;

b) základním rysem využívání [hromadných komunikačních údajů] [bezpečnostními a zpravodajskými službami] je odhalování dosud neznámých hrozeb pro národní bezpečnost prostřednictvím neadresných hromadných metod, které jsou závislé na shromažďování hromadných komunikačních údajů na jednom místě. Jeho hlavní užitečnost spočívá v rychlé identifikaci a vypracování profilu cílů, jakož i v poskytnutí základny pro činnost v případě bezprostředního ohrožení;

c) poskytovatel sítě elektronických komunikací nemá povinnost následně uchovávat [hromadné komunikační údaje] (nad rámec doby své obvyklé obchodní potřeby), které jsou tak uchovávány pouze státem ([bezpečnostními a zpravodajskými službami]);

d) vnitrostátní soud je názoru (s výhradou některých vyhrazených otázek), že záruky týkající se využívání [hromadných komunikačních údajů] [bezpečnostními a zpravodajskými službami] jsou v souladu s požadavky EÚLP, a

e) vnitrostátní soud je názoru, že při uplatnění podmínek stanovených v bodech 119 až 125 rozsudku [ze dne 21. prosince 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970)] by byla zmařena opatření přijatá [bezpečnostními a zpravodajskými službami] za účelem ochrany národní bezpečnosti, čímž by došlo k ohrožení národní bezpečnosti Spojeného království;

1) spadá požadavek v pokynu ministra adresovaném poskytovateli sítě elektronických komunikací, aby poskytl hromadné komunikační údaje bezpečnostním a zpravodajským službám členského státu, s ohledem na článek 4 SEU a čl. 1 odst. 3 směrnice [2002/58], do oblasti působnosti unijního práva a směrnice [2002/58]?

2) V případě kladné odpovědi na první otázku, bude se na takový pokyn ministra vztahovat kterákoli z podmínek [platných pro uchovávané komunikační údaje a upřesněných v bodech 119 až 125 rozsudku ze dne 21. prosince 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970)] nebo jakákoli jiná podmínka nad rámec podmínek stanovených EÚLP? A pokud ano, jak a v jakém rozsahu se

tyto podmínky uplatní, vzhledem k nezbytnosti využívání metod hromadného shromažďování a automatického zpracovávání [bezpečnostními a zpravodajskými službami] za účelem ochrany národní bezpečnosti a vzhledem k rozsahu, ve kterém tyto možnosti, jež jsou jinak v souladu s EÚLP, mohou být uplatněním takových podmínek kriticky oslabeny?“

K předběžným otázkám

K první otázce

30 Podstatou první otázky předkládajícího soudu je, zda musí být čl. 1 odst. 3 směrnice 2002/58 ve spojení s čl. 4 odst. 2 SEU vykládán v tom smyslu, že vnitrostátní právní úprava, která státnímu orgánu umožňuje uložit poskytovatelům služeb elektronických komunikací povinnost předávat bezpečnostním a zpravodajským službám – pro účely zajištění národní bezpečnosti – provozní a lokalizační údaje, spadá do oblasti působnosti této směrnice.

31 K tomu Privacy International v podstatě uvádí, že – s ohledem na závěry vyplývající z judikatury Soudního dvora k oblasti působnosti směrnice 2002/58 – shromažďování údajů bezpečnostními a zpravodajskými službami u těchto poskytovatelů na základě článku 94 zákona z roku 1984 i využívání těchto údajů uvedenými službami spadá do oblasti působnosti této směrnice, a to bez ohledu na to, zda jsou zmíněné údaje shromažďovány prostřednictvím následného předání, nebo v reálném čase. Konkrétně uvádí, že výslovné zmínění cíle ochrany národní bezpečnosti ve výčtu uvedeném v čl. 15 odst. 1 této směrnice nemá za následek nepoužitelnost této směrnice na takové situace a čl. 4 odst. 2 SEU nemá na tento závěr žádný dopad.

32 Naproti tomu vláda Spojeného království, česká a estonská vláda, Irsko, jakož i francouzská, kyperská, maďarská, polská a švédská vláda v podstatě tvrdí, že směrnice 2002/58 se na vnitrostátní právní úpravu dotčenou ve věci v původním řízení nevztahuje, protože účelem této právní úpravy je zajištění národní bezpečnosti. Činnosti bezpečnostních a zpravodajských služeb patří podle nich mezi základní funkce členských států související s udržováním veřejného pořádku a s ochranou vnitřní bezpečnosti a územní celistvosti, a tudíž spadají do jejich výhradních pravomocí, jak dosvědčuje zejména čl. 4 odst. 2 třetí věta SEU.

33 Směrnici 2002/58 proto podle těchto vlád nelze vykládat v tom smyslu, že by vnitrostátní opatření, jejichž cílem je zajištění národní bezpečnosti, spadala do oblasti její působnosti. Článek 1 odst. 3 této směrnice omezuje oblast její působnosti, ze které vylučuje – stejně jako stanovil již dříve čl. 3 odst. 2 první odrážka směrnice 95/46 – činnosti týkající se veřejné bezpečnosti, obrany a bezpečnosti státu. Tato ustanovení odrážejí rozdělení pravomocí stanovené v čl. 4 odst. 2 SEU a byla by zbavena užitečného účinku, kdyby opatření z oblasti národní bezpečnosti musela být v souladu s požadavky směrnice 2002/58. Dále uvádějí, že na čl. 1 odst. 3 směrnice 2002/58 lze vztáhnout judikaturu Soudního dvora vycházející z rozsudku ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346), týkajícího se čl. 3 odst. 2 první odrážky směrnice 95/46.

34 V této souvislosti je třeba uvést, že podle čl. 1 odst. 1 směrnice 2002/58 se touto směrnicí zejména harmonizují vnitrostátní právní předpisy požadované pro zajištění rovnocenné úrovně ochrany základních práv a svobod, zejména práva na soukromí a zachování důvěrnosti informací, se zřetelem na zpracování osobních údajů v odvětví elektronických komunikací.

35 Článek 1 odst. 3 této směrnice vylučuje z její působnosti „činnosti státu“ v oblastech, které jsou v něm uvedeny, včetně činností v oblasti trestního práva a činností týkajících se veřejné bezpečnosti, obrany, bezpečnosti státu a hospodářské prosperity státu, jedná-li se o činnosti související s bezpečností státu.

V této souvislosti jsou uvedené činnosti v každém případě příkladem činností státu či státních orgánů, které se liší od činnosti jednotlivců (rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 32 a citovaná judikatura).

36 Článek 3 směrnice 2002/58 dále stanoví, že se tato směrnice vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii, včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů (dále jen „služby elektronických komunikací“). Na uvedenou směrnici je tudíž třeba nahlížet tak, že upravuje činnosti poskytovatelů takových služeb (rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 33 a citovaná judikatura).

37 V tomto kontextu čl. 15 odst. 1 směrnice 2002/58 umožňuje členským státům přijímat za dodržení jím stanovených podmínek „legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice“ (rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 71).

38 Článek 15 odst. 1 směrnice 2002/58 přitom nutně počítá s tím, že v něm zmiňovaná vnitrostátní legislativní opatření spadají do oblasti její působnosti, jelikož tato směrnice výslovně umožňuje členským státům přijmout je pouze v případě, že splní v ní stanovené podmínky. Takovými opatřeními se dále pro účely, jež jsou uvedeny v tomto ustanovení, řídí činnost poskytovatelů služeb elektronických komunikací (rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 34 a citovaná judikatura).

39 Zejména s ohledem na tyto úvahy Soudní dvůr rozhodl, že čl. 15 odst. 1 ve spojení s článkem 3 směrnice 2002/58 musí být vykládán v tom smyslu, že do působnosti této směrnice spadá nejen legislativní opatření, které poskytovatelům služeb elektronických komunikací ukládá povinnost uchovávat provozní a lokalizační údaje, ale i legislativní opatření, které jim ukládá povinnost zpřístupnit tyto údaje příslušným vnitrostátním orgánům. Taková legislativní opatření totiž nutně znamenají, že tito poskytovatelé uvedené údaje zpracovávají, takže v rozsahu, v němž upravují činnosti uvedených poskytovatelů, nemohou být považována za činnosti vlastní státům ve smyslu čl. 1 odst. 3 uvedené směrnice (v tomto smyslu viz rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 35 a 37 a citovaná judikatura).

40 K takovému legislativnímu opatření, jako je článek 94 zákona z roku 1984, na jehož základě může příslušný orgán udělit poskytovatelům služeb elektronických komunikací pokyn zpřístupnit hromadné údaje přenosem bezpečnostním a zpravodajským službám, je třeba poznamenat, že podle definice uvedené v čl. 4 bodě 2 nařízení 2016/679 – která je použitelná na základě článku 2 směrnice 2002/58 ve spojení s čl. 94 odst. 2 uvedeného nařízení – se pojmem „zpracování osobních údajů“ označuje „jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, […] uložení, […] nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění […]“.

41 Z toho vyplývá, že zpřístupňování osobních údajů přenosem je, stejně jako ukládání údajů nebo jakékoliv jiné zpřístupnění, zpracováním ve smyslu článku 3 směrnice 2002/58, a tudíž spadá do oblasti působnosti této směrnice (v tomto smyslu viz rozsudek ze dne 29. ledna 2008, Promusicae, C-275/06, EU:C:2008:54, bod 45).

42 S ohledem na úvahy rozvedené výše v bodě 38 tohoto rozsudku a na celkovou systematiku směrnice 2002/58 by navíc takovým výkladem této směrnice, podle kterého by legislativní opatření uvedená v jejím čl. 15 odst. 1 byla v důsledku toho, že se účel takových opatření v podstatě kryje s účely sledovanými činnostmi, na které se vztahuje čl. 1 odst. 3 téže směrnice, vyloučena z oblasti její působnosti, byl citovaný čl. 15 odst. 1 zcela zbaven užitečného účinku (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 72 a 73).

43 Pojem „činnosti“ použitý v čl. 1 odst. 3 směrnice 2002/58 proto nelze, jak v podstatě podotkl generální advokát v bodě 75 svého stanoviska ve spojených věcech La Quadrature du Net a další (C-511/18 a C-512/18, EU:C:2020:6), na které odkazuje v bodě 24 svého stanoviska v projednávané věci, vykládat v tom smyslu, že zahrnuje i legislativní opatření uvedená v čl. 15 odst. 1 této směrnice.

44 Ustanovení čl. 4 odst. 2 SEU, kterých se dovolávají vlády zmíněné výše v bodě 32 tohoto rozsudku, nemohou tento závěr vyvrátit. Podle ustálené judikatury Soudního dvora totiž členským státům sice přísluší vymezit své podstatné bezpečnostní zájmy a přijmout opatření způsobilá k zajištění své vnitřní a vnější bezpečnosti, avšak na základě pouhé skutečnosti, že určité vnitrostátní opatření bylo přijato za účelem ochrany národní bezpečnosti, nelze vyloučit uplatnění unijního práva a zprostit členské státy povinnosti jej nutně dodržovat [v tomto smyslu viz rozsudky ze dne 4. června 2013, ZZ, C-300/11, EU:C:2013:363, bod 38 a citovaná judikatura; ze dne 20. března 2018, Komise v. Rakousko (Státní tiskárna), C-187/16, EU:C:2018:194, body 75 a 76, jakož i ze dne 2. dubna 2020, Komise v. Polsko, Maďarsko a Česká republika (Dočasný mechanismus relokace žadatelů o mezinárodní ochranu), C-715/17, C-718/17 a C-719/17, EU:C:2020:257, body 143 a 170].

45 Je pravda, že Soudní dvůr v rozsudku ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346, body 56 až 59), rozhodl, že předávání osobních údajů leteckými dopravci veřejným orgánům třetího státu za účelem předcházení terorismu a jiným závažným trestným činům a boje proti nim nespadá – na základě čl. 3 odst. 2 první odrážky směrnice 95/46 – do oblasti působnosti této směrnice, protože takové předávání spadá do rámce zavedeného orgány veřejné moci, jejichž cílem je veřejná bezpečnost.

46 Tuto judikaturu ovšem nelze – s ohledem na úvahy uvedené výše v bodech 36, 38 a 39 tohoto rozsudku – uplatnit na výklad čl. 1 odst. 3 směrnice 2002/58. Jak totiž v podstatě podotkl generální advokát v bodech 70 až 72 svého stanoviska ve spojených věcech La Quadrature du Net a další (C-511/18 a C-512/18, EU:C:2020:6), čl. 3 odst. 2 první odrážka směrnice 95/46, k němuž se citovaná judikatura vztahuje, obecně vylučoval z oblasti působnosti této směrnice „zpracování, které se týká veřejné bezpečnosti, obrany, bezpečnosti státu“, a nerozlišoval podle subjektu, který dotčené zpracování údajů provádí. Naproti tomu při výkladu čl. 1 odst. 3 směrnice 2002/58 se takové rozlišování ukazuje jako nezbytné. Jak totiž vyplývá z bodů 37 až 39 a 42 tohoto rozsudku, do oblasti působnosti uvedené směrnice spadá veškeré zpracovávání osobních údajů prováděné poskytovateli služeb elektronických komunikací, a tedy i zpracování, k němuž dochází v důsledku povinnosti uložené jim orgány veřejné moci, přestože na takové zpracování se – s ohledem na širší formulaci ustanovení čl. 3 odst. 2 první odrážky směrnice 95/46, která pokrývá každé zpracování, jehož předmětem je veřejná bezpečnost, obrana nebo bezpečnost státu, a to bez ohledu na subjekt, který takové zpracování provádí – případně mohla vztahovat výjimka stanovená v tomto ustanovení.

47 Kromě toho je třeba poukázat na to, že směrnice 95/46 dotčená ve věci, ve které byl vydán rozsudek ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346), byla článkem 94 odst. 1 nařízení 2016/679 zrušena a nahrazena tímtéž nařízením, a to s účinkem ode dne 25. května 2018. Citované nařízení přitom sice v čl. 2 odst. 2 písm. d) upřesňuje, že se nevztahuje na zpracování prováděné „příslušnými orgány“ za účelem mimo jiné prevence a odhalování trestných činů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, avšak z čl. 23 odst. 1 písm. d) a h) téhož nařízení vyplývá, že zpracování osobních údajů prováděné za těmito účely jednotlivci spadá do oblasti jeho působnosti. Z toho plyne, že shora popsaný výklad čl. 1 odst. 3, článku 3 a čl. 15 odst. 1 směrnice 2002/58 je v souladu s vymezením oblasti působnosti nařízení 2016/679, které tato směrnice doplňuje a upřesňuje.

48 Naproti tomu v případech, kdy členské státy přímo provádějí opatření odchylující se od zásady důvěrnosti elektronických komunikací, aniž poskytovatelům služeb takových komunikací uloží povinnosti zpracování, nespadá ochrana údajů subjektů údajů do působnosti směrnice 2002/58, nýbrž jen do působnosti vnitrostátního práva – s výhradou použití směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních

údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. 2016, L 119, s. 89) – takže dotčená opatření musí být v souladu zejména s vnitrostátním ústavním pořádkem a s požadavky EÚLP.

49 S ohledem na výše rozvedené úvahy je třeba na první otázku odpovědět, že čl. 1 odst. 3, článek 3 a čl. 15 odst. 1 směrnice 2002/58 ve spojení s čl. 4 odst. 2 SEU musí být vykládány v tom smyslu, že vnitrostátní právní úprava, která státnímu orgánu umožňuje uložit poskytovatelům služeb elektronických komunikací povinnost předávat bezpečnostním a zpravodajským službám – pro účely zajištění národní bezpečnosti – provozní a lokalizační údaje, spadá do oblasti působnosti této směrnice.

K druhé otázce

50 Podstatou druhé otázky předkládajícího soudu je, zda musí být čl. 15 odst. 1 směrnice 2002/58 ve spojení s čl. 4 odst. 2 SEU, jakož i s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která umožňuje státnímu orgánu uložit poskytovatelům služeb elektronických komunikací – pro účely zajištění národní bezpečnosti – povinnost plošného a nerozlišujícího předávání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám.

51 Předně je třeba připomenout, že podle informací uvedených v žádosti o rozhodnutí o předběžné otázce poskytuje článek 94 zákona z roku 1984 ministrovi oprávnění uložit poskytovatelům služeb elektronických komunikací formou pokynu povinnost, považuje-li to za nezbytné v zájmu národní bezpečnosti nebo v zájmu vztahů s cizí vládou, předat bezpečnostním a zpravodajským službám hromadné komunikační údaje zahrnující provozní a lokalizační údaje a informace o použitých službách ve smyslu čl. 21 odst. 4 a 6 RIPA. Toto posledně zmíněné ustanovení zahrnuje mimo jiné údaje nezbytné k identifikaci zdroje sdělení a jeho adresáta, ke zjištění data, času a doby trvání komunikace a k určení typu sdělení, k identifikaci použitého vybavení a ke zjištění polohy koncových zařízení a sdělení, tedy údaje, mezi něž patří mimo jiné jméno a adresa uživatele, telefonní čísla volajícího a volaného, adresa internetového protokolu (IP) zdroje a adresáta sdělení, jakož i adresy navštívených internetových stránek.

52 Takové zpřístupnění údajů přenosem se týká všech uživatelů prostředků elektronické komunikace a není upřesněno, zda má k tomuto přenosu docházet v reálném čase, nebo až následně. Podle informací uvedených v žádosti o rozhodnutí o předběžné otázce jsou tyto údaje po provedení přenosu uloženy bezpečnostními a zpravodajskými službami a zůstávají těmto službám k dispozici pro účely jejich činností, stejně jako jiné databáze v držení těchto služeb. Konkrétně mohou být takto shromážděné údaje, které jsou hromadně a automatizovaně zpracovávány a analyzovány, propojeny s jinými databázemi obsahujícími různé kategorie hromadných osobních údajů nebo zpřístupněny mimo tyto služby a do třetích států. Konečně tyto operace nepodléhají předchozímu povolení soudu nebo nezávislého správního orgánu a subjekty údajů o nich nejsou nijak informovány.

53 Účelem směrnice 2002/58 je, jak vyplývá zejména z bodů 6 a 7 jejího odůvodnění, ochránit uživatele služeb elektronických komunikací před riziky, která pro jejich osobní údaje a soukromí vyplývají z nových technologií, a zejména zvyšující se kapacity automatického uchovávání a zpracování údajů. Cílem této směrnice je v této souvislosti konkrétně, jak se uvádí v bodě 2 jejího odůvodnění, zajistit plné dodržování práv zakotvených v článcích 7 a 8 Listiny. V tomto ohledu z důvodové zprávy k návrhu směrnice Evropského parlamentu a Rady o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací [COM (2000) 385 final], z něhož vychází směrnice 2002/58, vyplývá, že záměrem unijního normotvůrce bylo „zachovat i nadále vysokou úroveň ochrany osobních údajů a soukromí u všech služeb elektronických komunikací bez ohledu na použitou technologii“.

54 Článek 5 odst. 1 směrnice 2002/58 pro tyto účely stanoví, že „[č]lenské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů“. V témže ustanovení je také zdůrazněno, že členské státy „[z]ejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1“, a upřesněno, že „[t]ento odstavec nebrání technickému uchovávání, které je nezbytné pro přenos sdělení, aniž by tím byla dotčena zásada důvěrnosti“.

55 V citovaném čl. 5 odst. 1 je tedy zakotvena zásada důvěrného charakteru jak elektronických sdělení, tak s nimi souvisejících provozních údajů, a plyne z něj zejména zákaz – uložený v zásadě všem vyjma uživatelů – uchovávat tato sdělení a tyto údaje bez souhlasu uživatele. Toto ustanovení se vzhledem k obecnosti svého znění vztahuje nevyhnutelně na všechny operace umožňující třetím osobám seznámit se se sděleními a s nimi souvisejícími údaji za účely odlišnými od přenosu sdělení.

56 Zákaz odposlouchávat sdělení a zachycovat s nimi související údaje stanovený v čl. 5 odst. 1 směrnice 2002/58 se tedy vztahuje na jakékoliv zpřístupnění provozních a lokalizačních údajů poskytovateli služeb elektronických komunikací orgánům veřejné moci, jako jsou bezpečnostní a zpravodajské služby, jakož i na uchovávání uvedených údajů těmito orgány bez ohledu na jejich následné využití.

57 Přijetím směrnice tedy unijní normotvůrce konkretizoval práva zakotvená v článcích 7 a 8 Listiny, takže uživatelé prostředků elektronické komunikace mohou v zásadě právem očekávat, že jejich komunikace a s ní související údaje zůstanou anonymní a nebude možné je zaznamenat bez jejich souhlasu (rozsudek ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, bod 109).

58 Článek 15 odst. 1 směrnice 2002/58 nicméně členským státům umožňuje zavést výjimky ze základní povinnosti zakotvené v čl. 5 odst. 1 této směrnice, a sice povinnosti zaručit důvěrnost osobních údajů, a z navazujících povinností stanovených zejména v článcích 6 a 9 uvedené směrnice, pokud takové omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému. Za tímto účelem mohou členské státy mimo jiné přijmout legislativní opatření umožňující uchovávání údajů po omezenou dobu na základě některého z těchto důvodů.

59 Možností odchýlit se od práv a povinností stanovených v článcích 5, 6 a 9 směrnice 2002/58 ovšem nemůže být odůvodněno, aby se výjimka ze základní povinnosti zajistit důvěrný charakter elektronických sdělení a s nimi souvisejících údajů, a zejména ze zákazu uchovávat tyto údaje výslovně stanoveného v článku 5 této směrnice, stala pravidlem (v tomto smyslu viz rozsudky ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 89 a 104, jakož i ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, bod 111).

60 Z článku 15 odst. 1 třetí věty směrnice 2002/58 dále vyplývá, že členské státy mohou přijmout legislativní opatření s cílem omezit rozsah práv a povinností uvedených v článcích 5, 6 a 9 této směrnice jen tehdy, jsou-li tato opatření v souladu s obecnými zásadami unijního práva, k nimž patří zásada proporcionality, a se základními právy zaručenými Listinou. Soudní dvůr v této souvislosti již rozhodl, že povinnost uložená poskytovatelům služeb elektronických komunikací členským státem prostřednictvím vnitrostátní právní úpravy spočívající v uchovávání provozních údajů pro účely jejich případného zpřístupnění příslušným vnitrostátním orgánům vyvolává otázky, jež se týkají dodržování nejen článku 7 Listiny, týkajícího se ochrany soukromého života, a článku 8 Listiny, týkajícího se ochrany osobních údajů, ale i článku 11 Listiny, který se týká svobody projevu (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 25 a 70, jakož i ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 91 a 92 a citovaná judikatura).

61 Tytéž otázky vyvstávají i u jiných druhů zpracování údajů, jako je jejich předávání jiným osobám než uživatelům nebo přístup k těmto údajům za účelem jejich využití [obdobně viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, body 122 a 123 a citovaná judikatura].

62 Při výkladu čl. 15 odst. 1 směrnice 2002/58 je proto třeba zohlednit význam nejen práva na respektování soukromého života zaručeného článkem 7 Listiny a práva na ochranu osobních údajů zaručeného jejím článkem 8, jak vyplývá z judikatury Soudního dvora, ale i práva na svobodu projevu, neboť toto základní právo zaručené v článku 11 Listiny je jedním ze základních pilířů demokratické a pluralitní společnosti a je součástí hodnot, na kterých je podle článku 2 SEU založena Unie (v tomto smyslu viz rozsudky ze dne 6. března 2001, Connolly v. Komise, C-274/99 P, EU:C:2001:127, bod 39, a ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 93 a citovaná judikatura).

63 Práva zakotvená v článcích 7, 8 a 11 Listiny se však neprojevují jako absolutní výsady, ale musí být nahlížena ve vztahu k jejich společenské funkci (v tomto smyslu viz rozsudek ze dne 16. července 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 172 a citovaná judikatura).

64 Jak totiž plyne z čl. 52 odst. 1 Listiny, Listina připouští omezení výkonu takových práv za předpokladu, že jsou tato omezení stanovena zákonem, respektují podstatu těchto práv a při dodržení zásady proporcionality jsou nezbytná a skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

65 K tomu je třeba doplnit, že požadavek, aby každé omezení výkonu základních práv bylo stanoveno zákonem, implikuje, že právní základ dovolující zásah do těchto práv musí sám definovat rozsah omezení výkonu dotyčného práva (rozsudek ze dne 16. července 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 175 a citovaná judikatura).

66 V souvislosti s dodržením zásady proporcionality čl. 15 odst. 1 první věta směrnice 2002/58 stanoví, že členské státy mohou přijmout opatření odchylující se od zásady důvěrnosti sdělení a s nimi souvisejících provozních údajů, pokud je takové opatření „v demokratické společnosti nezbytné, vhodné a přiměřené“ vzhledem k účelům uvedeným v tomto ustanovení. V bodě 11 odůvodnění této směrnice je upřesněno, že opatření této povahy musí být „plně“ přiměřené vzhledem k zamýšlenému účelu.

67 V tomto ohledu je třeba připomenout, že podle ustálené judikatury Soudního dvora ochrana základního práva na respektování soukromého života vyžaduje, aby výjimky z ochrany osobních údajů a omezení této ochrany byly činěny v mezích toho, co je nezbytně nutné. Kromě toho nelze při sledování cíle obecného zájmu nelze ztrácet ze zřetele skutečnost, že tento cíl je třeba uvést do souladu se základními právy dotčenými daným opatřením, a to vyváženým poměřením tohoto cíle s dotčenými právy a zájmy [v tomto smyslu viz rozsudky ze dne 16. prosince 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727, bod 56; ze dne 9. listopadu 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662, body 76, 77 a 86, jakož i ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, bod 52; posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 140].

68 Za účelem splnění požadavku proporcionality musí právní úprava stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a stanovit minimální požadavky, tak aby osoby, o jejichž osobní údaje jde, měly dostatečné záruky umožňující účinně chránit tyto údaje před rizikem zneužití. Tato právní úprava musí být právně závazná ve vnitrostátním právu a musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracovávání takových údajů, čímž zaručí, že se zásah omezí na to, co je nezbytně nutné. Potřeba takových záruk je o to významnější v případě, kdy jsou osobní údaje zpracovávány automaticky, zejména když existuje značné riziko neoprávněného přístupu k těmto údajům. Tyto úvahy platí zvláště tehdy, jedná-li se o ochranu oné konkrétní kategorie osobních údajů, jíž tvoří citlivé údaje [v tomto smyslu viz rozsudky ze dne 8. dubna 2014,

Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 54 a 55, jakož i ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 117; posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 141].

69 K otázce, zda je taková vnitrostátní právní úprava, jako je úprava dotčená ve věci v původním řízení, v souladu s požadavky čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, je třeba poznamenat, že předání provozních a lokalizačních údajů jiným osobám než uživatelům, například bezpečnostním a zpravodajským službám, představuje výjimku ze zásady důvěrnosti. Jestliže je taková operace prováděna, stejně jako v projednávané věci, plošně a nerozlišujícím způsobem, pak se z výjimky ze základní povinnosti zajistit důvěrný charakter údajů stává v jejím důsledku pravidlo, přestože systém zavedený směrnicí 2002/58 vyžaduje, aby taková výjimka zůstala výjimkou.

70 Kromě toho je podle ustálené judikatury Soudního dvora předávání provozních a lokalizačních údajů třetí straně zásahem do základních práv zakotvených v článcích 7 a 8 Listiny bez ohledu na následné využití těchto údajů. V tomto ohledu není důležité, zda dotyčné informace o soukromém životě představují citlivé údaje nebo zda dotyčné osoby utrpěly z důvodu tohoto zásahu případné nepříznivé následky [v tomto smyslu viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, body 124 a 126 a citovaná judikatura, jakož i rozsudek ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, body 115 a 116].

71 Takové předání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám představuje zásah do práva zakotveného v článku 7 Listiny, který musí být považován za zvlášť závažný, zejména s ohledem na citlivost informací, které z těchto údajů mohou vyplynout, a především na možnost vytvořit z nich profil subjektů údajů, neboť taková informace je stejně citlivé povahy, jako je samotný obsah sdělení. Navíc může v subjektech údajů vyvolávat dojem, že jejich soukromí je pod neustálým dohledem (obdobně viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 27 a 37, jakož i ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 99 a 100).

72 Dále je třeba poukázat na to, že předávání provozních a lokalizačních údajů orgánům veřejné moci pro bezpečnostní účely může být samo o sobě zásahem do práva na respektování komunikace zakotveného v článku 7 Listiny a odrazovat uživatele prostředků elektronické komunikace od výkonu jejich svobody projevu zaručené v článku 11 Listiny. Takové odrazující účinky přitom mohou mít dopad zejména na osoby, jejichž komunikace podléhá podle vnitrostátních předpisů profesnímu tajemství, a na oznamovatele, jejichž činnosti jsou chráněny směrnicí Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie (Úř. věst. 2019, L 305, s. 17). Tyto účinky jsou mimoto tím závažnější, čím větší je množství a rozmanitost ukládaných údajů (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, bod 28; ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 101, jakož i ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, bod 118).

73 Konečně s ohledem na značné množství provozních a lokalizačních údajů, které mohou být průběžně ukládány na základě opatření plošného ukládání, a na citlivou povahu informací, které z těchto údajů mohou vyplynout, vzniká riziko zneužití a neoprávněného přístupu již samotným uložením těchto údajů poskytovateli služeb elektronických komunikací.

74 Co se týče cílů, které by mohly odůvodnit takové zásahy, konkrétně cíle zajistit národní bezpečnost dotčeného ve věci v původním řízení, je třeba předeslat, že podle čl. 4 odst. 2 SEU zůstává národní bezpečnost výhradní odpovědností každého členského státu. Tato odpovědnost odpovídá prvořadému zájmu chránit základní funkce státu a základní zájmy společnosti a zahrnuje prevenci a represi činností, které by mohly silně destabilizovat základní ústavní, politické, hospodářské nebo společenské

uspořádání země, a zejména přímo ohrožovat společnost, obyvatelstvo nebo stát jako takový, jako jsou mimo jiné teroristické činnosti (rozsudek ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, bod 135).

75 Význam cíle zajistit národní bezpečnost, nahlíženého z hlediska čl. 4 odst. 2 SEU, přitom přesahuje význam ostatních cílů uvedených v čl. 15 odst. 1 směrnice 2002/58, zejména cíle bojovat proti obecné trestné, ač závažné činnosti, a cíle zajistit veřejnou bezpečnost. Takové hrozby, jako jsou hrozby uvedené v předchozím bodě, se totiž svou povahou a zvláštní závažnosti liší od obecného rizika vzniku napětí nebo narušování, ač závažného, veřejné bezpečnosti. Cílem zajistit národní bezpečnost tedy lze, jsou-li splněny ostatní požadavky stanovené v čl. 52 odst. 1 Listiny, odůvodnit opatření zasahující do základních práv závažněji než opatření, která by mohla být odůvodněna těmito ostatními cíli (rozsudek ze dne 6. října 2020, La Quadrature du Net a další, C-511/18, C-512/18 a C-520/18, bod 136).

76 Vnitrostátní právní úprava zasahující do základních práv zakotvených v článcích 7 a 8 Listiny musí ovšem k tomu, aby byla v souladu s požadavkem proporcionality – připomenutým výše v bodě 67 tohoto rozsudku, podle kterého musí být výjimky z ochrany osobních údajů a její omezení činěny v mezích toho, co je nezbytně nutné – splňovat požadavky vyplývající z judikatury citované výše v bodech 65, 67 a 68 tohoto rozsudku.

77 Konkrétně v souvislosti s přístupem orgánu k osobním údajům nestačí, když právní úprava pouze vyžaduje, aby přístup orgánů k těmto údajům odpovídal některému z cílů sledovanému touto právní úpravou, nýbrž musí rovněž stanovit hmotněprávní a procesní podmínky, jimiž se toto jejich využití bude řídit [obdobně viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 192 a citovaná judikatura].

78 Proto – a vzhledem k tomu, že obecný přístup ke všem uloženým údajům bez jakékoli, byť i nepřímé souvislosti se sledovaným cílem nelze považovat za omezený na to, co je nezbytně nutné – musí vnitrostátní právní úprava přístupu k provozním a lokalizačním údajům vycházet z objektivních kritérií, na jejichž základě jsou vymezeny okolnosti a podmínky, za nichž musí být příslušným vnitrostátním orgánům poskytnut přístup k dotčeným údajům (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 119 a citovaná judikatura).

79 Tyto požadavky tím spíše platí pro takové legislativní opatření, jako je opatření dotčené ve věci v původním řízení, na jehož základě může příslušný vnitrostátní orgán uložit poskytovatelům služeb elektronických komunikací povinnost plošně a nerozlišujícím způsobem zpřístupnit provozní a lokalizační údaje přenosem bezpečnostním a zpravodajským službám. V důsledku takového přenosu jsou totiž tyto údaje zpřístupněny orgánům veřejné moci [obdobně viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 212].

80 Předávání provozních a lokalizačních údajů se vzhledem k tomu, že k němu dochází plošně a nerozlišujícím způsobem, týká globálně všech osob, které využívají služeb elektronických komunikací. Vztahuje se tedy i na osoby, v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset s cílem zajistit národní bezpečnost, a především bez nutnosti prokázat souvislost mezi údaji, k jejichž předání má dojít, a hrozbou pro národní bezpečnost (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 57 a 58, jakož i ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 105). S ohledem na skutečnost, že předání takových údajů orgánům veřejné moci odpovídá – v souladu s konstatováním uvedeným výše v bodě 79 tohoto rozsudku – jejich zpřístupnění, je třeba dospět k závěru, že důsledkem právní úpravy umožňující plošné a nerozlišující předávání údajů orgánům veřejné moci je obecný přístup.

81 Z toho vyplývá, že vnitrostátní právní úprava, která poskytovatelům služeb elektronických komunikací ukládá povinnost plošně a nerozlišujícím způsobem zpřístupnit provozní a lokalizační údaje přenosem bezpečnostním a zpravodajským službám, překračuje meze toho, co je nezbytně nutné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje čl. 15 odst. 1 směrnice 2002/58 ve spojení s čl. 4 odst. 2 SEU, jakož i s články 7, 8 a 11 a čl. 52 odst. 1 Listiny.

82 S ohledem na výše rozvedené úvahy je třeba na druhou otázku odpovědět, že čl. 15 odst. 1 směrnice 2002/58 ve spojení s čl. 4 odst. 2 SEU, jakož i s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která umožňuje státnímu orgánu uložit poskytovatelům služeb elektronických komunikací – pro účely zajištění národní bezpečnosti – povinnost plošného a nerozlišujícího předávání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám.

K nákladům řízení

83 Vzhledem k tomu, že řízení má, pokud jde o účastníky původního řízení, povahu incidenčního řízení ve vztahu ke sporu probíhajícímu před předkládajícím soudem, je k rozhodnutí o nákladech řízení příslušný uvedený soud. Výdaje vzniklé předložením jiných vyjádření Soudnímu dvoru než vyjádření uvedených účastníků řízení se nenahrazují.

Z těchto důvodů Soudní dvůr (velký senát) rozhodl takto:

1) **Článek 1 odst. 3, článek 3 a čl. 15 odst. 1 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, ve spojení s čl. 4 odst. 2 SEU musí být vykládány v tom smyslu, že vnitrostátní právní úprava, která státnímu orgánu umožňuje uložit poskytovatelům služeb elektronických komunikací povinnost předávat bezpečnostním a zpravodajským službám – pro účely zajištění národní bezpečnosti – provozní a lokalizační údaje, spadá do oblasti působnosti této směrnice.**

2) **Článek 15 odst. 1 směrnice 2002/58, ve znění směrnice 2009/136, ve spojení s čl. 4 odst. 2 SEU, jakož i s články 7, 8 a 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která umožňuje státnímu orgánu uložit poskytovatelům služeb elektronických komunikací – pro účely zajištění národní bezpečnosti – povinnost plošného a nerozlišujícího předávání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám.**

Podpisy