



Sbírka soudních rozhodnutí

ROZSUDEK SOUDNÍHO DVORA (velkého senátu)

6. října 2020 *

[znění opravené usnesením ze dne 16. listopadu 2020]

Obsah

Právní rámec	6
Unijní právo	6
Směrnice 95/46	6
Směrnice 97/66	7
Směrnice 2000/31	7
Směrnice 2002/21	8
Směrnice 2002/58	9
Nařízení 2016/679	12
Francouzské právo	16
Zákoník vnitřní bezpečnosti	16
CPCE	20
Zákon č. 2004-575 ze dne 21. června 2004 o posílení důvěry v digitální ekonomiku	22
Nařízení vlády č. 2011-219	23
Belgické právo	25
Spory v původních řízeních a předběžné otázky	26
Věc C-511/18	26
Věc C-512/18	29

* Jednací jazyk: francouzština

Věc C-520/18	30
K řízení před Soudním dvorem	31
K předběžným otázkám	31
K prvním otázkám ve věcech C-511/18 a C-512/18, jakož i k první a druhé otázce ve věci C-520/18 ...	31
Úvodní poznámky	32
K oblasti působnosti směrnice 2002/58	33
K výkladu čl. 15 odst. 1 směrnice 2002/58	35
– K legislativním opatřením stanovícím preventivní uchovávání provozních a lokalizačních údajů za účelem zajištění národní bezpečnosti	40
– K legislativním opatřením stanovícím preventivní uchovávání provozních a lokalizačních údajů pro účely boje proti trestné činnosti a zajištění veřejné bezpečnosti	41
– K legislativním opatřením stanovícím preventivní uchovávání IP adres a údajů o totožnosti občanů pro účely boje proti trestné činnosti a zajištění veřejné bezpečnosti	43
– K legislativním opatřením stanovícím urychlené uchování provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti	44
Ke druhé a třetí otázce ve věci C-511/18	46
K automatizované analýze provozních a lokalizačních údajů	47
Ke shromažďování provozních a lokalizačních údajů v reálném čase	49
K vyrozumění subjektů, jejichž údaje byly shromažďovány nebo analyzovány	50
Ke druhé otázce ve věci C-512/18	51
Ke třetí otázce ve věci C-520/18	54
K nákladům řízení	56

„Řízení o předběžné otázce – Zpracování osobních údajů v odvětví elektronických komunikací – Poskytovatelé služeb elektronických komunikací – Poskytovatelé hostingových služeb a poskytovatelé přístupu k internetu – Plošné a nerozlišující uchovávání provozních a lokalizačních údajů – Automatizovaná analýza dat – Přístup k datům v reálném čase – Zajištění národní bezpečnosti a boj proti terorismu – Boj proti trestné činnosti – 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 – Směrnice 2000/31/ES – Oblast působnosti – Listina základních práv Evropské unie – Články 4, 6 až 8 a 11 a čl. 52 odst. 1 – Článek 4 odst. 2 SEU“

Ve spojených věcech C-511/18, C-512/18 a C-520/18,

jejichž předmětem jsou žádosti o rozhodnutí o předběžné otázce na základě článku 267 SFEU, podané rozhodnutími Conseil d'État (Státní rada, Francie) ze dne 26. července 2018, došlými Soudnímu dvoru dne 3. srpna 2018 (C-511/18 a C-512/18), a rozhodnutím Cour constitutionnelle (Ústavní soud, Belgie) ze dne 19. července 2018, došlým Soudnímu dvoru dne 2. srpna 2018 (C-520/18), v řízeních

La Quadrature du Net (C-511/18 a C-512/18),

French Data Network (C-511/18 a C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 a C-512/18),

Igwan.net (C-511/18),

proti

Premier ministre (C-511/18 a C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 a C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), za účasti:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

a

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

proti

Conseil des ministres,

za účasti:

Child Focus (C-520/18),

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 jednání konaném ve dnech 9. a 10. září 2019,

s ohledem na vyjádření předložená:

- za La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net a Center for Democracy and Technology A. Fitzjean Ō Cobhthaighem, avocat,
- za French Data Network Y. Padovou, avocat,
- za Privacy International H. Royem, avocat,
- za Ordre des barreaux francophones et germanophone E. Kiehl, P. Limbrée, E. Lemmensem, A. Cassartem a J.-F. Henrottem, avocats,
- za Académie Fiscale ASBL a UA J.-P. Riquetem,
- za Liga voor Mensenrechten ASBL J. Vander Velpenem, avocat,
- za Ligue des Droits de l'Homme ASBL, J. Jespersem a J. Fermonem, avocats,
- za VZ, WY a XX D. Pattynem, avocat,
- za Child Focus N. Buisseret, K. De Meesterem a J. Van Cauterem avocats,
- za francouzskou vládu původně D. Duboisem, F. Alabrunem, D. Colasem, E. de Moustier a A.-L. Desjonquères, poté D. Duboisem, F. Alabrunem, E. de Moustier a A.-L. Desjonquères, jako zmocněnci,
- za belgickou vládu J.-C. Halleuxem, P. Cottinem a C. Pochet, jako zmocněnci, ve spolupráci s J. Vanpraetem, Y. Peetersem, S. Deprém a E. de Lophemem, avocats,
- za českou vládu M. Smolkem, J. Vláčilem a O. Serdulou, jako zmocněnci,
- za dánskou vládu původně J. Nymann-Lindegrenem, M. Wolff a P. Ngo, poté J. Nymann-Lindegrenem a M. Wolff, jako zmocněnci,
- za německou vládu původně J. Möllerem, M. Hellmannem, E. Lankenauem, R. Kanitzem a T. Henzem, poté J. Möllerem, M. Hellmannem, E. Lankenauem a R. Kanitzem, jako zmocněnci,
- za estonskou vládu N. Grünberg a A. Kalbus, jako zmocněnkyněmi,
- za irskou vládu A. Joycem, M. Browne a G. Hodge, jako zmocněnci, ve spolupráci s D. Fennellym, BL,

- za španělskou vládu původně L. Aguilera Ruizem a A. Rubio Gonzálezem, poté L. Aguilera Ruizem, jako zmocněncem,
- za kyperskou vládu E. Neofytou, jako zmocněnkyní,
- za lotyšskou vládu V. Šoneca, jako zmocněnkyní,
- za maďarskou vládu původně M. Z. Fehérem a Z. Wagner, poté M. Z. Fehérem, jako zmocněncem,
- za nizozemskou vládu M. K. Bulterman a M. A. M. de Ree, jako zmocněnkyněmi,
- za polskou vládu B. Majczynou, J. Sawickou a M. Pawlickou, jako zmocněnci,
- za švédskou vládu původně H. Shev, H. Eklinder, C. Meyer-Seitz a A. Falk, poté H. Shev, H. Eklinder, C. Meyer-Seitz a J. Lundberg, jako zmocněnkyněmi,
- za vládu Spojeného království S. Brandonem, jako zmocněncem, ve spolupráci s G. Facennou, QC, a C. Knightem, barrister,
- [odrážka odstraněna usnesením ze dne 16. listopadu 2020],
- za Evropskou komisi původně H. Kranenborgem, M. Wasmeierem a P. Costa de Oliveira, poté H. Kranenborgem a M. Wasmeierem, 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 Žádosti o rozhodnutí o předběžné otázce se týkají výkladu 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“), a článků 12 až 15 směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) (Úř. věst. 2000, L 178, s. 1; Zvl. vyd. 13/02, s. 399), ve spojení s články 4, 6 až 8 a 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“) a s čl. 4 odst. 2 SEU.
- 2 Žádost ve věci C-511/18 byla předložena v rámci sporů mezi La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs a Igwan.net na jedné straně a Premier ministre (předseda vlády, Francie), Garde des Sceaux, ministre de la justice (ministr spravedlnosti, Francie), ministre de l'Intérieur (ministr vnitra, Francie) a ministre des Armées (ministr obrany, Francie) na druhé straně ohledně legality décret n° 2015-1885 du 28 septembre 2015, portant désignation des services spécialisés de renseignement (nařízení vlády č. 2015-1185 ze dne 28. září 2015, o určení specializovaných zpravodajských služeb) (JORF ze dne 29. září 2015, text 1 z 97, dále jen „nařízení vlády č. 2015-1185“), décret n° 2015-1211 du 1^{er} octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (nařízení vlády č. 2015-1211 ze dne 1. října 2015, o žalobách ve věcech použití

zpravodajských metod podléhajících povolení a evidencí týkajících se bezpečnosti státu) (JORF ze dne 2. října 2015, text 7 ze 108, dále jen „nařízení vlády č. 2015-1211“), décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure (nařízení vlády č. 2015-1639 ze dne 11. prosince 2015, o určení jiných než specializovaných zpravodajských služeb oprávněných používat metody uvedené v hlavě V části VIII zákoníku vnitřní bezpečnosti) (JORF ze dne 12. prosince 2015, text 28 ze 127, dále jen „nařízení vlády č. 2015-1639“) a décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (nařízení vlády č. 2016-67 ze dne 29. ledna 2016, o zpravodajských metodách sběru informací) (JORF ze dne 31. ledna 2016, text 2 ze 113, dále jen „nařízení vlády č. 2016-67“).

- 3 Žádost ve věci C-512/18 byla předložena v rámci sporů mezi French Data Network, La Quadrature du Net a Fédération des fournisseurs d'accès à Internet associatifs na jedné straně a Premier ministre (předseda vlády, Francie) a Garde des Sceaux, ministre de la justice (ministr spravedlnosti, Francie) na druhé straně ohledně legality článku R. 10-13 code des postes et des communications électroniques (zákoník poštovních služeb a elektronických komunikací) (dále jen „CPCE“) a décret n° 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (nařízení vlády č. 2011-219 ze dne 25. února 2011, o uchovávání a sdělování údajů umožňujících určit totožnost každé osoby, která přispěla k vytváření obsahu nabízeného on-line) (JORF ze dne 1. března 2011, text 32 ze 170, dále jen „nařízení vlády č. 2011-219“).
- 4 Žádost ve věci C-520/18 byla předložena v rámci sporů mezi Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY a XX na jedné straně a Conseil des ministres (rada ministrů, Belgie) na druhé straně ohledně legality loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zákon ze dne 29. května 2016, o shromažďování a uchovávání údajů v odvětví elektronických komunikací) (*Moniteur belge* ze dne 18. července 2016, s. 44717, dále jen „zákon ze dne 29. května 2016“).

Právní rámec

Unijní právo

Směrnice 95/46

- 5 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 ode dne 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 (Úř. věst. 2016, L 119, s. 1; oprava Úř. věst. 2018, L 127, s. 2). Článek 3 odst. 2 směrnice 95/46 stanovil:

„Tato směrnice se nevztahuje na zpracování osobních údajů:

- prováděné pro výkon činností, které nespádají do oblasti působnosti práva Společenství a jsou uvedeny [které nespádají do oblasti působnosti práva Společenství, jako jsou činnosti uvedené] v hlavě V a VI Smlouvy o Evropské unii, 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.“

- 6 Článek 22 směrnice 95/46, obsažený v její kapitole III, nadepsané „Soudní přezkum, odpovědnost a sankce“, zněl takto:

„Aniž je tím dotčena možnost opravného prostředku ve správním řízení, který je možno podat, zejména orgánu dozoru uvedenému v článku 28, stanoví všechny členské státy, že každá osoba má právo v případě porušení práv, jež jí jsou zaručeny vnitrostátními předpisy, které se uplatní na dotčené zpracování, předložit věc soudu.“

Směrnice 97/66

- 7 Článek 5 směrnice Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. 1997, L 24, s. 1), nadepsaný „Důvěrný charakter sdělení“, stanovil:

„1. Členské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných telekomunikačních služeb. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 14 odst. 1.

2. Odstavec 1 se nedotýká v souladu se zákonem povoleného zaznamenávání sdělení, je-li prováděno v rámci zákonných obchodních praktik za účelem prokazování obchodních transakcí nebo jakéhokoli jiného sdělení v rámci podnikatelských činností.“ *(neoficiální překlad)*

Směrnice 2000/31

- 8 Body 14 a 15 odůvodnění směrnice 2000/31 znějí:

„(14) Ochrana fyzických osob při zpracování osobních údajů je výhradně upravena směrnicí [95/46] a směrnicí [97/66], které se plně uplatní pro služby informační společnosti. Tyto směrnice již vytvářejí právní rámec Společenství pro oblast osobních údajů a není tedy nezbytné pro zajištění řádného fungování vnitřního trhu, a zejména volného pohybu osobních údajů mezi členskými státy, upravovat tuto otázku v této směrnici. Provádění a uplatňování této směrnice musí být v souladu se zásadami ochrany osobních údajů, zejména pokud jde o nevyžádaná obchodní sdělení a odpovědnost zprostředkovatelů. Tato směrnice nemůže bránit anonymnímu užívání otevřených sítí, jako je internet.

(15) Důvěrnost komunikace je zaručena článkem 5 směrnice [97/66]. V souladu s touto směrnicí zakazují členské státy všechny typy protiprávního zadržování nebo sledování komunikace jinými osobami, než je odesílatel a příjemce, ledaže jsou tyto činnosti podle práva povolené.“

- 9 Článek 1 směrnice 2000/31 zní takto:

„1. Cílem této směrnice je přispět k řádnému fungování vnitřního trhu tím, že zajistí volný pohyb služeb informační společnosti mezi členskými státy.

2. Je-li to pro dosažení cíle uvedeného v odstavci 1 potřebné, dbá tato směrnice o sblížení některých vnitrostátních ustanovení platných pro služby informační společnosti, která se týkají vnitřního trhu, usazování poskytovatelů služeb, obchodních sdělení, elektronických smluv, odpovědnosti zprostředkovatelů, kodexů chování, mimosoudního urovnávání sporů, soudních postupů [prostředků soudní ochrany] a spolupráce mezi členskými státy.

3. Tato směrnice doplňuje právo Společenství platné pro služby informační společnosti, aniž je dotčena úroveň ochrany, zejména v oblasti veřejného zdraví a zájmů spotřebitelů, jak vyplývá z právních nástrojů Společenství a vnitrostátních právních předpisů, které je provádějí, nebude-li tím omezen volný pohyb služeb informační společnosti.

[...]

5. Tato směrnice se nevztahuje na:

[...]

b) otázky týkající se služeb informační společnosti upravené ve směrnících [95/46] a [97/66];

[...]“

10 Článek 2 směrnice 2000/31 zní:

„Pro účely této směrnice se rozumí:

a) ‚službami informační společnosti‘: služby ve smyslu čl. 1 odst. 2 směrnice [Evropského Parlamentu a Rady] 98/34/ES [ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů (Úř. věst. 1998, L 204, s. 37; Zvl. vyd. 13/20, s. 337)] ve znění směrnice [Evropského parlamentu a Rady] 98/48/ES [ze dne 20. července 1998 (Úř. věst. 1998, L 217, s. 18; Zvl. vyd. 13/21, s. 8)];

[...]“

11 Článek 15 směrnice 2000/31 stanoví:

„1. Členské státy neukládají poskytovatelům služeb uvedených v člancích 12, 13 a 14 obecnou povinnost dohlížet na jimi přenášené nebo ukládané informace nebo obecnou povinnost aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní činnost.

2. Členské státy mohou poskytovatelům služeb informační společnosti uložit povinnost, aby neprodleně informovali příslušné orgány veřejné moci o pravděpodobných protiprávních činnostech vykonávaných poskytovateli [příjemci jejich služeb] služeb nebo o protiprávních informacích, které tito poskytovatelé [příjemci] poskytují, nebo aby sdělili příslušným orgánům veřejné moci na jejich žádost informace, na jejichž základě lze zjistit totožnost příjemců jejich služeb, s nimiž uzavřeli dohodu o shromažďování informací.“

Směrnice 2002/21

12 Bod 10 odůvodnění směrnice 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) uvádí:

„Definice ‚služby informační společnosti‘ v článku 1 směrnice [98/34], ve znění směrnice [98/48] zahrnuje širokou škálu hospodářských činností, které probíhají on-line. Většina těchto činností nespadá do oblasti působnosti této směrnice, protože nespočívají zcela nebo převážně v přenášení signálů po sítích elektronických komunikací. Tato směrnice se vztahuje na hlasové telefonní služby a služby přenosu elektronické pošty. Tým podnik, například poskytovatel služby Internetu, může nabízet jak služby elektronických komunikací, jako je například přístup na Internet, tak služby, na které se tato směrnice nevztahuje, jako je poskytování obsahu využívající Internet.“

13 Článek 2 směrnice 2002/21 stanoví:

„Pro účely této směrnice se:

[...]

- c) „službou elektronických komunikací“ rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové vysílání, s výjimkou služeb poskytujících obsah nebo vykonávajících redakční dohled nad obsahem přenášeným prostřednictvím sítí a služeb elektronických komunikací; pojem nezahrnuje služby informační společnosti, jak jsou definovány v článku 1 směrnice [98/34], které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací;

[...]“

Směrnice 2002/58

14 Body 2, 6, 7, 11, 22, 26 a 30 odůvodnění směrnice 2002/58 uvádějí:

- „(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 člancích 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 možnostmi, 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. [...]

[...]

- (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 [...] 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. [...]"

15 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 nespádají 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.“

16 Článek 2 směrnice 2002/58, nadepsaný „Definice“, stanoví:

„Není-li stanoveno jinak, použijí se definice uvedené ve směrnici [95/46] a směrnici [2002/21].

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 rozumí 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 účastníkovi nebo uživateli, který tyto informace přijímá;

[...]“

- 17 Článek 3 směrnice 2002/58, 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 ve Společenství, včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů.“

- 18 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.“

- 19 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.“

- 20 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 obdržetím 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. [...]“

- 21 Článek 15 uvedené směrnice, nadepsaný „Použití některých ustanovení směrnice [95/46]“, stanoví:

„1. 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.

[...]

2. Ustanovení směrnice [95/46], kapitoly III o soudním přezkumu, odpovědnosti a sankcích, se použijí s ohledem na vnitrostátní právní předpisy přijaté v souladu s touto směrnicí a s ohledem na práva jednotlivců vyplývající z této směrnice.

[...]“

Nařízení 2016/679

- 22 V bodě 10 odůvodnění nařízení 2016/679 se uvádí:

„S cílem zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci Unie by měla být úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním těchto údajů rovnocenná ve všech členských státech. V celé Unii je třeba zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. [...]“

23 Článek 2 tohoto nařízení 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.

[...]

4. Tímto nařízením není dotčeno uplatňování směrnice [2000/31], zejména pokud jde o pravidla týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb uvedená v člancích 12 až 15 uvedené směrnice.“

24 Článek 4 uvedeného nařízení stanoví:

„Pro účely tohoto nařízení se rozumí:

- 1) ‚osobními údaji‘ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů‘); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
- 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;

[...]“

25 Článek 5 nařízení 2016/679 stanoví:

„1. Osobní údaje musí být:

- a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (‚zákonnost, korektnost a transparentnost‘);
- b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely (‚účelové omezení‘);

- c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“;
- d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“;
- e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);
- f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

[...]“

26 Článek 6 tohoto nařízení zní:

„1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

[...]

- c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

[...]

3. Základ pro zpracování podle odst. 1 písm. c) a e) musí být stanoven:

- a) právem Unie nebo;
- b) právem členského státu, které se na správce vztahuje.

Účel zpracování musí vycházet z tohoto právního základu [...] Tento právní základ může obsahovat konkrétní ustanovení pro přizpůsobení uplatňování tohoto nařízení, včetně obecných podmínek, kterými se řídí zákonnost zpracování správcem, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupů zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace, při nichž dochází ke zpracování, než stanoví kapitola IX. Právo Unie nebo členského státu musí splňovat cíl veřejného zájmu a musí být přiměřené sledovanému legitimnímu cíli.

[...]“

27 Článek 23 uvedeného nařízení stanoví:

„1. Právo Unie nebo členského státu, které se na správce nebo zpracovatele vztahuje, může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v člancích 12 až 22 a v článku 34, jakož i v článku 5, v rozsahu, v jakém ustanovení tohoto článku odpovídají právům

a povinností stanoveným v člancích 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 a 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) ochranu subjektu údajů nebo práv a svobod druhých;
- j) vymáhání občanskoprávních nároků.

2. Každé legislativní opatření uvedené v odstavci 1 zejména obsahuje konkrétní ustanovení, alespoň, je-li to relevantní, pokud jde o:

- a) účely zpracování nebo kategorie zpracování;
- b) kategorie osobních údajů;
- c) rozsah zavedených omezení;
- d) záruky proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání;
- e) specifikaci správců nebo kategorie správců;
- f) doby uložení a platné záruky s ohledem na povahu, rozsah a účely zpracování nebo kategorie zpracování;
- g) rizika z hlediska práv a svobod subjektů údajů; a
- h) právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na účelu účelu omezení.“

28 Článek 79 odst. 1 uvedeného nařízení stanoví:

„Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.“

29 Článek 94 nařízení 2016/679 stanoví:

„1. Směrnice [95/46] se zrušuje s účinkem ode dne 25. května 2018.

2. 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.“

30 Článek 95 tohoto nařízení stanoví:

„Toto nařízení neukládá žádné další povinnosti fyzickým nebo právnickým osobám, pokud jde o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii, co se týče záležitostí, u nichž se na ně vztahují konkrétní povinnosti s tímž cílem stanovené ve směrnici [2002/58].“

Francouzské právo

Zákoník vnitřní bezpečnosti

31 Část VIII legislativní části code de la sécurité intérieure (zákoník vnitřní bezpečnosti; dále jen „CSI“) stanoví v člancích L. 801-1 až L. 898-1 pravidla týkající se informací.

32 Článek L. 811-3 CSI stanoví:

„Zvláštní zpravodajské služby mohou výhradně k plnění svých příslušných úkolů použít metody uvedené v hlavě V této části ke shromažďování informací týkajících se obrany a prosazování následujících hlavních národních zájmů:

1. národní nezávislost, územní celistvost a národní obrana;
2. zásadní zájmy zahraniční politiky, plnění evropských a mezinárodních závazků Francie a předcházení všem formám zahraničního vměšování;
3. významné hospodářské, průmyslové a vědecké zájmy Francie;
4. předcházení terorismu;
5. předcházení:
 - a) zásahům do republikánského uspořádání orgánů;
 - b) činnostem směřujícím k zachování nebo k obnově uskupení rozpuštěných na základě článku L. 212-1;
 - c) kolektivnímu násilí, které by mohlo vážně narušit veřejný pořádek;
6. předcházení organizované trestné činnosti a organizovanému zločinu;
7. předcházení šíření zbraní hromadného ničení.“

33 Článek L. 811-4 stanoví:

„Nařízení vlády přijaté na základě stanoviska Conseil d'État [(Státní rada, Francie)] a po vydání stanoviska Commission nationale de contrôle des techniques de renseignement [(Národní komise pro kontrolu zpravodajských metod, Francie)] určí služby, které nejsou zvláštními zpravodajskými

službami, spadající pod ministry obrany, vnitra a spravedlnosti, jakož i ministry pro hospodářství, rozpočet nebo cla, kterým může být povoleno použít metody uvedené v hlavě V této části za podmínek stanovených v téže části. Pro každou službu konkretizuje účely uvedené v článku L. 811–3 a metody, které mohou být předmětem povolení.“

34 Článek L. 821-1 první pododstavec CSI upřesňuje:

„Použití metod shromažďování informací uvedených v kapitolách I až IV hlavy V této části v tuzemsku podléhá předchozímu povolení předsedy vlády vydanému po vydání stanoviska Národní komise pro kontrolu zpravodajských metod.“

35 Článek L. 821-2 CSI stanoví:

„Povolení uvedené v článku L. 821-1 se vydává na základě písemné a odůvodněné žádosti ministra obrany, ministra vnitra, ministra spravedlnosti nebo ministrů pro hospodářství, rozpočet nebo cla. Každý z ministrů může delegovat tuto pravomoc individuálně pouze na přímé spolupracovníky prověřené pro tajemství v zájmu národní obrany.

V žádosti se uvede:

1. metoda nebo metody, které mají být použity;
2. služba, pro kterou je žádost podána;
3. sledovaný účel nebo účely;
4. odůvodnění opatření;
5. doba platnosti povolení;
6. dotčené osoby, místa nebo vozidla.

Pro účely použití bodu 6 mohou být osoby, jejichž totožnost není známa, označeny svými identifikátory nebo vlastnostmi a místa nebo vozidla mohou být označena odkazem na osoby, které jsou předmětem žádosti.

[...]“

36 Článek L. 821-3 první pododstavec CSI stanoví:

„Žádost se předloží předsedovi nebo, není-li to možné, jednomu z členů Národní komise pro kontrolu zpravodajských metod uvedených v bodech 2 a 3 článku L. 831-1, který vydá stanovisko pro předsedu vlády do dvaceti čtyř hodin. Je-li žádost posuzována užším kolegiem nebo plénem komise, je o tom předseda vlády neprodleně informován a stanovisko je vydáno do sedmdesáti dvou hodin.“

37 Článek L. 821-4 CSI stanoví:

„Povolení k použití metod uvedených v kapitolách I až IV hlavy V této části vydává předseda vlády na dobu nejvýše čtyř měsíců. [...] Povolení obsahuje odůvodnění a údaje uvedené v bodech 1 až 6 článku L. 821-2. Každé povolení lze prodloužit za stejných podmínek, jaké jsou stanoveny v této kapitole.

Je-li povolení vydáno i přes nepříznivé stanovisko Národní komise pro kontrolu zpravodajských metod, uvedou se v něm důvody, proč nebylo tomuto stanovisku vyhověno.

[...]“

38 Článek L. 833-4 CSI obsažený v kapitole III této hlavy stanoví:

„Z vlastní iniciativy nebo na základě stížnosti jakékoli osoby, která si přeje ověřit, že vůči ní není neoprávněně používána žádná zpravodajská metoda, provede komise kontrolu uvedené metody nebo metod za účelem ověření, že byly nebo jsou používány v souladu s touto částí. Komise sdělí stěžovateli, že byla provedena nezbytná ověření, aniž potvrdí či vyvrátí použití zpravodajských metod.“

39 Článek L. 841-1 první a druhý pododstavec CSI zní takto:

„S výhradou zvláštních ustanovení článku L. 854-9 tohoto zákoníku je k rozhodování o žalobách týkajících se použití zpravodajských metod uvedených v hlavě V této části příslušná Conseil d'État [(Státní rada)] za podmínek stanovených v kapitole III hlavy VII části VII code de justice administrative [(zákoník správního soudnictví)].

Žalobu může podat:

1. každá osoba, která si přeje ověřit, že vůči ní nejsou neoprávněně použity žádné zpravodajské metody, a která prokáže předchozí využití postupu stanoveného v článku L. 833-4;

2. Národní komise pro kontrolu zpravodajských metod za podmínek stanovených v článku L. 833-8.“

40 Součástí hlavy V části VIII legislativní části CSI, týkající se „metod shromažďování informací podléhajících povolení“, je mimo jiné kapitola I nadepsaná „Přístup správních orgánů k údajům o připojení“, která obsahuje články L. 851-1 až L. 851-7 CSI.

41 Článek L. 851-1 CSI stanoví:

„Za podmínek stanovených v kapitole I hlavy II této části může být u provozovatelů elektronických komunikací a osob uvedených v článku L. 34-1 [CPCE], jakož i osob uvedených v bodech 1 a 2 odst. I článku 6 loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(zákon č. 2004-575 ze dne 21. června 2004 o posílení důvěry v digitální ekonomiku; JORF ze dne 22. června 2004, s. 11168)] povoleno shromažďování informací či dokumentů zpracovávaných nebo uchovávaných prostřednictvím jejich sítí nebo služeb elektronických komunikací, včetně technických údajů týkajících se identifikace účastnických nebo připojovacích čísel ke službám elektronických komunikací, evidence všech účastnických nebo připojovacích čísel určené osoby, umístění použitého koncového zařízení a komunikace účastníka v podobě seznamu volaných a volajících čísel, doby trvání a data komunikace.

Odchylně od článku L. 821-2 jsou písemné a odůvodněné žádosti týkající se technických údajů o identifikaci účastnických nebo připojovacích čísel ke službám elektronických komunikací či evidence všech účastnických nebo připojovacích čísel určené osoby předávány přímo Národní komisi pro kontrolu zpravodajských metod osobami individuálně určenými a zmocněnými zpravodajskými službami, které jsou uvedeny v člancích L. 811-2 a L. 811-4. Komise vydá stanovisko za podmínek stanovených v článku L. 821-3.

Útvar předsedy vlády odpovídá za shromažďování informací nebo dokumentů od provozovatelů a osob uvedených v prvním pododstavci tohoto článku. Národní komise pro kontrolu zpravodajských metod má stálý, úplný, přímý a okamžitý přístup ke shromážděným informacím nebo dokumentům.

Prováděcí pravidla k tomuto článku se stanoví nařízením vlády přijatým na základě stanoviska Státní rady a po vydání stanoviska Commission nationale de l'informatique et des libertés [(Národní komise pro informační technologie a svobody, Francie)] a Národní komise pro kontrolu zpravodajských metod.“

42 Článek L. 851-2 CSI stanoví:

„I. Za podmínek stanovených v kapitole I hlavy II této části a pouze pro účely předcházení terorismu může být na sítích provozovatelů a osob uvedených v článku L. 851-1 jednotlivě povoleno shromažďování informací nebo dokumentů uvedených v témže článku L. 851-1, které se týkají předem identifikované osoby, u níž lze předpokládat, že může mít vazbu na určitou hrozbu, a to v reálném čase. Existují-li závažné důvody se domnívat, že jedna nebo více osob, které patří do okolí osoby dotčené povolením, může poskytnout informace s ohledem na účel, který odůvodňuje povolení, může být toto povolení rovněž uděleno jednotlivě ve vztahu ke každé z těchto osob.

I *bis*. Nejvyšší počet současně platných povolení vydaných na základě tohoto článku stanoví předseda vlády po vydání stanoviska Národní komise pro kontrolu zpravodajských metod. Rozhodnutí o stanovení této kvóty a jejím rozdělení mezi ministry uvedené v prvním pododstavci článku L. 821-2, jakož i počet vydaných povolení k zachycování informací se oznámí komisi.

[...]“

43 Článek L. 851-3 CSI stanoví:

„I. – Za podmínek stanovených v kapitole I hlavy II této části a pouze pro účely předcházení terorismu může být provozovatelům a osobám uvedeným v článku L. 851-1 uloženo, aby na svých sítích zavedli automatizované zpracování k identifikování spojení, která mohou odhalit hrozbu terorismu, a to v závislosti na parametrech uvedených v povolení.

Toto automatizované zpracování používá výlučně informace nebo dokumenty uvedené v článku L. 851-1, aniž jsou shromažďovány jiné údaje než ty, které splňují nastavené parametry, a aniž lze identifikovat osoby, ke kterým se informace nebo dokumenty vztahují.

V souladu se zásadou proporcionality musí být v povolení předsedy vlády upřesněn technický rozsah provádění tohoto zpracování.

II. – Národní komise pro kontrolu zpravodajských metod vydá stanovisko k žádosti o povolení týkající se automatizovaného zpracování a nastavených detekčních parametrů. Komise má trvalý, úplný a přímý přístup k tomuto zpracování, jakož i ke shromážděným informacím a údajům. Je informována o veškerých změnách zpracování a parametrů a může vydávat doporučení.

První povolení k provádění automatizovaného zpracování podle bodu I tohoto článku se vydává na dobu dvou měsíců. Povolení lze prodloužit za časových podmínek stanovených v kapitole I hlavy II této části. Žádost o prodloužení obsahuje přehled o počtu identifikátorů hlášených automatizovaným zpracováním a analýzu relevance těchto hlášení.

III. – Podmínky stanovené v článku L. 871-6 se použijí na konkrétní operace uskutečňované při těchto činnostech provozovateli a osobami uvedenými v článku L. 851-1.

IV. – Pokud zpracování uvedené v bodě I tohoto článku odhalí údaje, které mohou nasvědčovat existenci hrozby teroristické povahy, může předseda vlády nebo některá z jím pověřených osob, po vydání stanoviska Národní komise pro kontrolu zpravodajských metod za podmínek stanovených v kapitole I hlavy II této části, povolit identifikaci dotčené osoby nebo osob a shromažďování

souvisejících údajů. Tyto údaje se využijí do šedesáti dnů od shromáždění, po jejichž uplynutí jsou zničeny, s výjimkou případů, kdy závažné důkazy potvrzují existenci teroristické hrozby spojené s jednou nebo více dotčenými osobami.

[...]“

44 Článek L. 851-4 CSI zní:

„Za podmínek stanovených v kapitole I hlavy II této části mohou být technické údaje o umístění použitých koncových zařízení uvedené v článku L. 851-1 shromážděny požadavkem na síť a provozovatelé je mohou v reálném čase předat útvaru předsedy vlády.“

45 Článek R. 851-5 CSI, který je součástí prováděcí části tohoto zákoníku, stanoví:

„I. – Informacemi nebo dokumenty uvedenými v článku L. 851-1 jsou s výjimkou obsahu vyměňované korespondence nebo vyhledávaných informací:

1. informace nebo dokumenty vyjmenované v člancích R. 10-13 a R. 10-14 [CPCE] a v článku 1 nařízení vlády [č. 2011-219];

2. technické údaje jiné než ty, které jsou uvedeny v bodě 1, a:

- a) umožňující určit místo, kde se nacházejí koncová zařízení;
- b) týkající se přístupu koncových zařízení k sítím nebo k veřejným komunikačním službám on-line;
- c) týkající se přenosu elektronických sdělení po sítích;
- d) týkající se identifikace a autentizace uživatele, připojení, sítě nebo veřejné komunikační služby on-line;
- e) týkající se vlastností koncových zařízení a konfiguračních údajů jejich softwaru.

II. – Na základě článku L. 851-1 lze shromažďovat pouze informace a dokumenty uvedené v odst. I bodě 1. K tomuto shromažďování dochází následně.

Informace uvedené v odst. I bodě 2 mohou být shromažďovány pouze na základě článků L. 851-2 a L. 851-3 za podmínek a omezení stanovených těmito články a s výhradou použití článku R. 851-9.“

CPCE

46 Článek L. 34-1 CPCE stanoví:

„I. – Tento článek se vztahuje na zpracování osobních údajů při poskytování služeb elektronických komunikací veřejnosti; vztahuje se zejména na sítě, které podporují zařízení pro shromažďování a identifikaci údajů.

II. – Aniž jsou dotčena ustanovení odstavců III, IV, V a VI, provozovatelé elektronických komunikací, a zejména osoby, jejichž činností je poskytování přístupu k veřejným komunikačním službám on-line, vymažou nebo anonymizují veškeré provozní údaje.

Osoby, které veřejnosti poskytují služby elektronických komunikací, zavedou v souladu s ustanoveními předchozího pododstavce vnitřní postupy pro vyřizování žádostí příslušných orgánů.

Osoby, které v rámci své hlavní nebo vedlejší profesní činnosti nabízejí veřejnosti připojení umožňující on-line komunikaci prostřednictvím přístupu do sítě, a to i bezúplatně, musí dodržovat předpisy, které se na základě tohoto článku použijí na provozovatele elektronických komunikací.

III. – Pro účely vyšetřování, odhalování a stíhání trestných činů nebo porušení povinnosti uvedené v článku L. 336-3 code de la propriété intellectuelle [(zákoník duševního vlastnictví)] nebo pro účely prevence útoků na systémy automatizovaného zpracovávání údajů uvedených v člancích 323-1 až 323-3-1 code pénal [(trestní zákoník)] a stíhání podle těchto článků a výhradně za účelem umožnit v případě potřeby poskytnutí informací justičnímu orgánu, Vysokému úřadu podle článku L. 331-12 zákoníku duševního vlastnictví nebo národnímu úřadu pro bezpečnost informačních systémů podle článku L. 2321-1 code de la défense [(zákoník obrany)] mohou být po dobu nejvýše jednoho roku odloženy úkony směřující k vymazání nebo k anonymizaci určitých kategorií technických údajů. Nařízením vlády přijatým na základě stanoviska Conseil d'État [(Státní rada)] a po vydání stanoviska Národní komise pro informační technologie a svobody se v mezích stanovených odstavcem VI určí tyto kategorie údajů a doba, po kterou jsou uchovávány, v závislosti na činnosti provozovatelů a na povaze sdělení, jakož i pravidla náhrady případných dodatečných identifikovatelných a specifických nákladů vzniklých provozovatelům v souvislosti se službami poskytnutými k tomuto účelu na žádost státu.

[...]

VI. – Údaje uchovávané a zpracováváné za podmínek stanovených v odstavcích III, IV a V se týkají výlučně identifikace uživatelů služeb poskytovaných provozovateli, technických charakteristik komunikace zajišťované těmito provozovateli a umístění koncových zařízení.

V žádném případě se nemohou týkat obsahu, a to v jakékoli podobě, korespondence vyměňované nebo informací vyhledávaných v rámci této komunikace.

Údaje jsou uchovávány a zpracovávány v souladu s ustanoveními loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(zákon č. 78-17 ze dne 6. ledna 1978 o výpočetní technice, evidencích a svobodách)].

Provozovatelé učiní vše pro to, aby zabránili použití těchto údajů k jiným účelům než k účelům stanoveným v tomto článku.“

47 Článek R. 10-13 CPCE zní takto:

„I. – Podle čl. L. 34-1 odst. III provozovatelé elektronických komunikací uchovávají pro účely vyšetřování, odhalování a stíhání trestných činů:

- a) informace umožňující identifikovat uživatele;
- b) údaje o použitých koncových zařízeních pro komunikaci;
- c) technické charakteristiky, jakož i datum, čas a dobu trvání každé komunikace;
- d) údaje o vyžádaných nebo využívaných doplňkových službách a jejich poskytovatelích;
- e) údaje umožňující identifikovat adresáta nebo adresáty sdělení.

II. – U telefonních služeb provozovatel uchovává údaje uvedené v odstavci II a také údaje umožňující identifikovat zdroj a umístění komunikace.

III. – Doba uchovávání údajů uvedených v tomto článku činí jeden rok ode dne, kdy byly zaznamenány.

IV. – Identifikovatelné a specifické dodatečné náklady vynaložené provozovateli, od kterých justiční orgány požadují údaje spadající do kategorií uvedených v tomto článku, se nahrazují za podmínek stanovených v článku R. 213-1 code de procédure pénale [(trestní řád)].“

48 Článek R. 10-14 CPCE stanoví:

„I. – Podle čl. L. 34-1 odst. IV jsou provozovatelé elektronických komunikací oprávněni uchovávat pro účely vyúčtování a plateb údaje technické povahy umožňující identifikovat uživatele, jakož i údaje uvedené v čl. R. 10-13 odst. I písm. b), c) a d).

II. – U telefonních služeb mohou provozovatelé uchovávat vedle údajů uvedených v odstavci I i údaje technické povahy týkající se umístění komunikace, identifikace adresáta nebo adresátů sdělení a údaje umožňující sestavit vyúčtování.

III. – Údaje uvedené v odstavcích I a II tohoto článku mohou být uchovávány pouze v případě, že jsou nezbytné pro vyúčtování a platbu za poskytnuté služby. Jejich uchovávání se musí omezit na dobu nezbytně nutnou pro tento účel a ne delší než jeden rok.

IV. – Pro účely bezpečnosti sítí a zařízení si mohou provozovatelé ponechat na dobu ne delší než tři měsíce:

- a) údaje umožňující identifikovat zdroj sdělení;
- b) technické charakteristiky, jakož i datum, čas a dobu trvání každé komunikace;
- c) údaje technické povahy umožňující identifikovat adresáta nebo adresáty sdělení;
- d) údaje týkající se požadovaných nebo použitých doplňkových služeb a jejich poskytovatelů.“

Zákon č. 2004-575 ze dne 21. června 2004 o posílení důvěry v digitální ekonomiku

49 Článek 6 zákona č. 2004-575 ze dne 21. června 2004 o posílení důvěry v digitální ekonomiku (JORF ze dne 22. června 2004, s. 11168, dále jen „LCEN“) stanoví:

„I. – 1. Osoby, jejichž činností je poskytování přístupu k veřejným komunikačním službám on-line, informují své účastníky o existenci technických prostředků umožňujících omezit přístup k některým službám nebo provést jejich výběr a nabídnou jim alespoň jeden z těchto prostředků.

[...]

2. Fyzické nebo právnické osoby, které i bezúplatně nabízejí veřejnosti veřejné komunikační služby on-line, ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb, nenesou občanskoprávní odpovědnost za činnosti nebo informace uložené na žádost příjemce těchto služeb, pokud tyto osoby skutečně nevěděly o jejich protiprávní povaze nebo o skutečnostech a okolnostech poukazujících na jejich protiprávní povahu, nebo pokud bezodkladně učinily kroky ke stažení nebo znepřístupnění těchto údajů, jakmile se o protiprávní povaze dozvěděly.

[...]

II. – Osoby uvedené v odst. I bodech 1 a 2 drží a uchovávají údaje, na jejichž základě lze zjistit totožnost kohokoli, kdo přispěl k vytváření obsahu nebo části obsahu poskytovaných služeb.

Poskytují osobám, které provozují veřejnou komunikační službu on-line, technické prostředky, které jim umožní splnit podmínky identifikování stanovené v odstavci III.

Justiční orgán může od poskytovatelů uvedených v odst. I bodech 1 a 2 požadovat sdělení údajů uvedených v prvním pododstavci.

Na zpracování těchto údajů se použijí ustanovení článků 226-17, 226-21 a 226-22 trestního zákoníku.

Nářízením vlády přijatým na základě stanoviska Státní rady a po vydání stanoviska Národní komise pro informační technologie a svobody se vymezí údaje uvedené v prvním pododstavci a určí doba a způsob jejich uchovávání.

[...]“

Nářízení vlády č. 2011-219

50 Kapitola I nařízení vlády č. 2011-219, přijatého na základě čl. 6 odst. II posledního pododstavce LCEN, obsahuje články 1 až 4 tohoto nařízení.

51 Článek 1 nařízení vlády č. 2011-219 stanoví:

„Údaje uvedené v čl. 6 odst. II [LCEN], které jsou osoby povinny uchovávat na základě tohoto ustanovení, jsou následující:

1. pro osoby uvedené v bodě 1 odst. I téhož článku a pro každé připojení jejich účastníků:

- a) identifikátor připojení;
- b) identifikátor přidělený účastníkovi těmito osobami;
- c) identifikátor koncového zařízení použitého k připojení, pokud k němu mají přístup;
- d) datum a čas zahájení a ukončení připojení;
- e) charakteristiky účastnického vedení;

2. pro osoby uvedené v odst. I bodě 2 téhož článku a pro každou tvůrčí operaci:

- a) identifikátor připojení u zdroje komunikace;
- b) identifikátor přidělený obsahu, jenž je předmětem operace;
- c) typy protokolů použitých pro připojení ke službě a pro přenos obsahu;
- d) povaha operace;
- e) datum a čas operace;
- f) identifikátor použitý autorem operace, pokud jej tento poskyt;

3. pro osoby uvedené v odst. I bodech 1 a 2 téhož článku informace poskytnuté uživatelem při uzavření smlouvy nebo při vytvoření účtu:

- a) identifikátor připojení při vytváření účtu;
- b) jméno a příjmení nebo firma;
- c) příslušné poštovní adresy;
- d) použité pseudonymy;
- e) příslušné adresy elektronické pošty nebo účtu;
- f) telefonní čísla;
- g) heslo a údaje umožňující jej ověřit nebo změnit, v jejich poslední aktualizované verzi;

4. pro osoby uvedené v odst. I bodech 1 a 2 téhož článku, je-li uzavření smlouvy nebo otevření účtu zpoplatněno, následující informace týkající se platby, a to pro každou platební transakci:

- a) druh provedené platby;
- b) reference platby;
- c) částka;
- d) datum a čas transakce.

Údaje uvedené v bodech 3 a 4 musí být uchovávány pouze tehdy, pokud je osoby obvykle shromažďují.“

52 Článek 2 tohoto nařízení vlády zní:

„Přispění k vytváření obsahu zahrnuje operace spočívající v:

- a) původním vytváření obsahu;
- b) změně obsahu a údajů souvisejících s obsahem;
- c) odstraňování obsahu.“

53 Článek 3 uvedeného nařízení vlády stanoví:

„Doba uchovávání údajů uvedených v článku 1 činí jeden rok:

- a) ode dne vytvoření obsahu pro každou operaci přispívající k vytvoření obsahu, jak je definována v článku 2, a to pro údaje uvedené v bodech 1 a 2;
- b) ode dne ukončení smlouvy nebo uzavření účtu, a to pro údaje uvedené v bodě 3;
- c) ode dne vystavení faktury pro každou fakturu nebo ode dne nebo platební operace pro každou platební operaci, a to pro údaje uvedené v bodě 4.“

Belgické právo

54 Zákonem ze dne 29. května 2016 byl změněn zejména loi du 13 juin 2005 relative aux communications électroniques (zákon ze dne 13. června 2005 o elektronických komunikacích; *Moniteur belge* ze dne 20. června 2005, s. 28070, dále jen „zákon ze dne 13. června 2005“), code d'instruction criminelle (trestní řád) a loi du 30 novembre 1998 organique des services de renseignement et de sécurité (organický zákon ze dne 30. listopadu 1998 o zpravodajských a bezpečnostních službách; *Moniteur belge* ze dne 18. prosince 1998, s. 40312, dále jen „zákon ze dne 30. listopadu 1998“).

55 Článek 126 zákona ze dne 13. června 2005, ve znění zákona ze dne 29. května 2016, stanoví:

„1. Aniž je dotčen loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (zákon ze dne 8. prosince 1992 o ochraně soukromí v souvislosti se zpracováním osobních údajů), poskytovatelé veřejně dostupných telefonních služeb, a to i prostřednictvím internetu, služeb připojení k internetu, služeb internetové elektronické pošty, provozovatelé veřejných elektronických komunikačních sítí, jakož i provozovatelé poskytující některou z těchto služeb uchovávají údaje uvedené v odstavci 3, které jsou jimi vytvářeny nebo zpracovávány při poskytování příslušných komunikačních služeb.

Tento článek se nevztahuje na obsah sdělení.

Povinnost uchovávat údaje uvedené v odstavci 3 se vztahuje rovněž na neúspěšná volání, pokud jsou tyto údaje v souvislosti s poskytováním dotčených komunikačních služeb:

- 1) vytvářené nebo zpracováváné provozovateli veřejně dostupných služeb elektronických komunikací nebo veřejné sítě elektronických komunikací, pokud se jedná o údaje o telefonování, nebo
- 2) evidované těmito poskytovateli, pokud se jedná o internetové údaje.

2. Pouze následující orgány mohou na žádost získat od poskytovatelů nebo provozovatelů uvedených v odst. 1 prvním pododstavci údaje uchovávané na základě tohoto článku pro tyto účely a za těchto podmínek:

- 1) soudní orgány za účelem odhalování, vyšetřování a stíhání trestných činů k provedení opatření stanovených v člancích 46 *bis* a 88 *bis* trestního řádu a za podmínek v nich stanovených;
- 2) zpravodajské a bezpečnostní služby za účelem plnění zpravodajských úkolů za použití metod sběru údajů uvedených v člancích 16/2, 18/7 a 18/8 organického zákona ze dne 30. listopadu 1998 o zpravodajských a bezpečnostních službách a za podmínek stanovených tímto zákonem;
- 3) každý příslušník soudní policie z Institut [belge des services postaux et des télécommunications (Belgický institut poštovních a telekomunikačních služeb, Belgie)] za účelem odhalování, vyšetřování a stíhání porušení článků 114, 124 a tohoto článku;
- 4) záchranné služby poskytující pomoc na místě, neobdrží-li v návaznosti na tísňové volání od příslušného poskytovatele nebo provozovatele identifikační údaje volajícího pomocí databáze uvedené v čl. 107 odst. 2 třetím pododstavci nebo obdrží-li neúplné nebo nesprávné údaje. Lze žádat pouze o identifikační údaje volajícího, a to nejpozději do 24 hodin od hovoru;
- 5) příslušník soudní policie z Cellule des personnes disparues de la Police Fédérale [(jednotka pro pohřešované osoby Federální policie, Belgie)] při poskytování pomoci osobě v ohrožení a při pátrání po osobách, jejichž zmizení budí obavy, a existují-li přesvědčivé domněnky či indicie o tom, že je bezprostředně ohrožena tělesná integrita pohřešované osoby. Od příslušného

provozovatele nebo poskytovatele lze prostřednictvím policejního oddělení určeného Králem žádat pouze o údaje uvedené v odst. 3 prvním a druhém pododstavci, které se týkají pohřešované osoby a byly uchovány během 48 hodin před podáním žádosti o poskytnutí údajů;

- 6) Service de médiation pour les télécommunications [(mediační služba pro telekomunikace, Belgie)] za účelem zjištění totožnosti osoby, která využila síť nebo službu elektronických komunikací zlovolně, a to v souladu s podmínkami stanovenými v čl. 43a odst. 3 bodě 7 loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (zákon ze dne 21. března 1991 o reformě některých veřejných hospodářských podniků). Lze žádat pouze o identifikační údaje.

Poskytovatelé a provozovatelé uvedení v odst. 1 prvním pododstavci zajistí, aby údaje uvedené v odstavci 3 byly z Belgie neomezeně přístupné a aby mohly být tyto údaje a všechny ostatní nezbytné informace týkající se těchto údajů neprodleně poskytnuty pouze orgánům uvedeným v tomto odstavci.

Nestanoví-li jiný právní předpis jinak, poskytovatelé a provozovatelé uvedení v odst. 1 prvním pododstavci nemohou použít údaje uchovávané na základě odstavce 3 k jiným účelům.

3. Údaje k identifikaci uživatele nebo účastníka a komunikačních prostředků, s výjimkou údajů konkrétně stanovených ve druhém a třetím pododstavci, se uchovávají po dobu dvanácti měsíců ode dne, kdy je komunikace prostřednictvím používané služby naposledy možná.

Údaje o přístupu a připojení koncového zařízení k síti nebo službě a o umístění tohoto zařízení, včetně koncového bodu sítě, se uchovávají po dobu dvanácti měsíců ode dne uskutečnění komunikace.

Komunikační údaje, s vyloučením obsahu, včetně údajů o zdroji a adresátovi sdělení, se uchovávají po dobu dvanácti měsíců ode dne uskutečnění komunikace.

Král vyhláškou schválenou Radou ministrů na návrh ministra spravedlnosti a ministra [příslušného pro záležitosti elektronických komunikací] a po vydání stanoviska Commission de la protection de la vie privée [(Komise pro ochranu soukromí, Belgie)] a Institutem stanoví druhy údajů dle kategorií uvedených v prvním až třetím pododstavci, které mají být uchovávány, a požadavky, které musí tyto údaje splňovat.

[...]"

Spory v původních řízeních a předběžné otázky

Věc C-511/18

- 56 Podáními ze dne 30. listopadu 2015 a 16. března 2016, která byla ve věci v původním řízení spojena, předložily La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs a Igwan.net ke Conseil d'État (Státní rada, Francie) návrh na zrušení nařízení vlády č. 2015-1185, 2015-1211, 2015-1639 a 2016-67 s odůvodněním, že jsou v rozporu zejména s francouzskou ústavou, evropskou Úmluvou o ochraně lidských práv a základních svobod (dále jen „EÚLP“), jakož i se směrnicemi 2000/31 a 2002/58, vykládanými ve světle článků 7, 8 a 47 Listiny.
- 57 Co se týče konkrétně žalobních důvodů vycházejících z porušení směrnice 2000/31, předkládající soud uvádí, že ustanovení článku L. 851-3 CSI ukládají provozovatelům elektronických komunikací a technickým poskytovatelům „povinnost zavést na svých sítích automatizované procesy určené, v závislosti na parametrech uvedených v povolení, k odhalování připojení, která by mohla ukazovat na hrozbu terorismu“. Cílem této metody je pouze po omezenou dobu shromažďovat ze všech údajů

o připojení zpracovávaných těmito provozovateli a poskytovateli ty údaje, které by mohly mít spojitost s takovým závažným protiprávním jednáním. Za těchto podmínek uvedená ustanovení, která neukládají obecnou povinnost aktivního dohledu, nejsou v rozporu s článkem 15 směrnice 2000/31.

- 58 Co se týče žalobních důvodů vycházejících z porušení směrnice 2002/58, předkládající soud má za to, že zejména z ustanovení této směrnice, jakož i 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), vyplývá, že vnitrostátní ustanovení ukládající poskytovatelům služeb elektronických komunikací takové povinnosti, jako je plošné a nerozlišující uchovávání provozních a lokalizačních údajů jejich uživatelů a účastníků, pro účely uvedené v čl. 15 odst. 1 uvedené směrnice, mezi které patří zajištění národní bezpečnosti, obrany a veřejné bezpečnosti, spadají do působnosti téže směrnice, pokud tyto právní předpisy upravují činnost uvedených poskytovatelů. Totéž platí pro právní předpisy upravující přístup vnitrostátních orgánů k údajům, jakož i jejich využití.
- 59 Předkládající soud z toho vyvozuje, že do působnosti směrnice 2002/58 spadá jak povinnost uchovávat údaje vyplývající z článku L. 851-1 CSI, tak přístup správních orgánů k uvedeným údajům, včetně přístupu v reálném čase upraveného v článcích L. 851-1, L. 851-2 a L. 851-4 uvedeného zákoníku. Totéž podle tohoto soudu platí i pro ustanovení článku L. 851-3 téhož zákoníku, která sice neukládají dotyčným provozovatelům obecnou povinnost uchovávání, avšak ukládají jim povinnost zavést na svých sítích automatizované procesy určené k odhalování spojení, která by mohla ukazovat na hrozbu terorismu.
- 60 Tento soud má naproti tomu za to, že do působnosti směrnice 2002/58 nespádají ta ustanovení CSI uvedená v návrzích na zrušení, která se týkají metod shromažďování informací prováděných přímo státem, přičemž neupravují činnosti poskytovatelů služeb elektronických komunikací uložením zvláštních povinností. Na tato ustanovení tedy nelze nahlížet tak, že provádějí unijní právo, tudíž se nelze úspěšně dovolávat žalobních důvodů vycházejících z jejich rozporu se směrnicí 2002/58.
- 61 Pro účely rozhodnutí o sporech týkajících se legality nařízení vlády č. 2015-1185, 2015-1211, 2015-1639 a 2016-67 vzhledem ke směrnici 2002/58 v rozsahu, v němž byla přijata k provedení článků L. 851-1 až L. 851-4 CSI, vyvstávají tedy tři otázky týkající se výkladu unijního práva.
- 62 Co se týče výkladu čl. 15 odst. 1 směrnice 2002/58, předkládající soud si zaprvé klade otázku, zda povinnost plošného a nerozlišujícího uchovávání uložená poskytovatelům služeb na základě článků L. 851-1 a R. 851-5 CSI nemůže být zejména s ohledem na záruky a kontroly, se kterými je spojen přístup správních orgánů k údajům o připojení a jejich využívání, považována za zásah odůvodněný právem na bezpečnost, které je zaručeno článkem 6 Listiny, a požadavky na národní bezpečnost, která je odpovědností samotných členských států na základě článku 4 SFEU.
- 63 Pokud jde zadruhé o ostatní povinnosti, které mohou být uloženy poskytovatelům služeb elektronických komunikací, předkládající soud poukazuje na to, že ustanovení článku L. 851-2 CSI dovolují shromažďovat informace nebo dokumenty uvedené v článku L. 851-1 tohoto zákoníku od týchž osob pouze pro účely předcházení terorismu. Toto shromažďování, jež se týká pouze jednoho nebo několika jednotlivců, kteří byli dříve identifikováni jako osoby, jež mohou mít vazbu na hrozbu terorismu, probíhá v reálném čase. Totéž platí pro ustanovení článku L. 851-4 uvedeného zákoníku, která opravňují k tomu, aby provozovatelé předávali v reálném čase pouze technické údaje týkající se umístění koncových zařízení. Tyto metody upravují pro odlišné účely a za odlišných prováděcích podmínek přístup správních orgánů k údajům uchovávaným na základě CPCE a LCEN v reálném čase, aniž na dotyčné poskytovatele kladou ve vztahu k uchovávání údajů požadavky přesahující to, co je nezbytné pro účtování a poskytování jejich služeb. Stejně tak ani ustanovení článku L. 851-3 CSI, která stanoví povinnost poskytovatelů služeb zavést na svých sítích automatizovanou analýzu připojení, nezahrnuje plošné a nerozlišující uchovávání údajů.

- 64 Předkládající soud má přitom za to, že jak plošné a nerozlišující uchovávání údajů o připojení, tak přístup k těmto údajům v reálném čase představují v kontextu vyznačujícím se vážnými a trvajících hrozbami pro národní bezpečnost, které spočívají zejména v nebezpečí terorismu, s ničím nesrovnatelný operativní přínos. Plošné a nerozlišující uchovávání totiž umožňuje zpravodajským službám přístup k údajům o komunikaci před tím, než jsou zjištěny důvody pro závěr, že dotyčná osoba představuje hrozbu pro veřejnou bezpečnost, obranu nebo bezpečnost státu. Kromě toho přístup k údajům o připojení v reálném čase umožňuje sledovat chování jednotlivců, kteří mohou představovat bezprostřední hrozbu pro veřejný pořádek, a velmi pružně na ně reagovat.
- 65 Metoda upravená v článku L. 851-3 CSI umožňuje dále na základě kritérií přesně definovaných za tímto účelem odhalit jednotlivce, jejichž jednání může, s ohledem na způsob jejich komunikace, odhalit hrozbu terorismu.
- 66 Zatřetí, pokud jde o přístup příslušných orgánů k uchovávaným údajům, předkládající soud se táže, zda směrnice 2002/58, nahlížená ve světle Listiny, musí být vykládána v tom smyslu, že v každém případě podmiňuje řádnost postupů shromažďování údajů o připojení požadavkem na vyrozumění subjektů údajů v případě, že taková informace již nemůže ohrozit vyšetřování vedené příslušnými orgány, nebo zda lze mít za to, že takové postupy jsou s ohledem na všechny ostatní procesní záruky stanovené vnitrostátním právem v souladu s právem, pokud tyto záruky zajišťují účinnost práva na opravný prostředek.
- 67 K těmto dalším procesním zárukám předkládající soud zejména upřesňuje, že každá osoba, která si přeje ověřit, že vůči ní není neoprávněně používána žádná zpravodajská metoda, se může obrátit na specializované kolegium Státní rady, kterému přísluší ověřit – s ohledem na skutečnosti, které jsou mu sděleny mimo sporné řízení – zda byla ve vztahu k žadateli použita některá z metod a zda k tomu došlo v souladu s částí VIII CSI. Pravomoci, které má toto kolegium k projednání žádostí, zaručují účinnost jím vykonávaného soudního přezkumu. V této souvislosti má pravomoc prošetřovat žádosti, zabývat se z úřední povinnosti všemi zjištěnými protiprávnostmi a nařizovat správním orgánům, aby přijaly veškerá vhodná opatření k nápravě zjištěných protiprávností. Kromě toho přísluší Národní komisi pro kontrolu zpravodajských metod ověřovat, že metody shromažďování informací jsou na vnitrostátním území prováděny v souladu s požadavky vyplývajícími z CSI. Okolnost, že právní předpisy dotčené ve věci v původním řízení neupravují vyrozumění dotčených osob o tom, že byly sledovány, tak sama o sobě nepředstavuje nepřiměřený zásah do práva na respektování soukromého života.
- 68 Za těchto podmínek se Conseil d'État (Státní rada) rozhodla přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:
- „1) Je třeba na povinnost plošného a nerozlišujícího uchovávání uloženou poskytovatelům na základě zmocňujících ustanovení čl. 15 odst. 1 směrnice [2002/58] nahlížet v kontextu vážného a trvajících ohrožení národní bezpečnosti, a zejména rizika terorismu tak, že jde o zásah odůvodněný právem na bezpečnost, které je zaručeno článkem 6 [Listiny], a požadavky národní bezpečnosti, za kterou podle článku 4 [SFEU] nesou odpovědnost výlučně členské státy?
 - 2) Musí být směrnice [2002/58] nahlížená ve světle [Listiny] vykládána v tom smyslu, že dovoluje taková legislativní opatření, jako jsou opatření pro shromažďování údajů o provozu a lokalizaci určitých jednotlivců reálném čase, která mají současně dopad na práva a povinnosti poskytovatelů služeb elektronických komunikací, ale neukládají jim zvláštní povinnost uchovávání údajů?
 - 3) Musí být směrnice [2002/58] nahlížená ve světle [Listiny] vykládána v tom smyslu, že v každém případě váže legalitu postupů shromažďování údajů o připojení na požadavek vyrozumět subjekty údajů, jakmile již není možné ohrozit probíhající vyšetřování vedené příslušnými orgány, nebo takové postupy mohou být považovány za legální s ohledem na všechny ostatní stávající procesní záruky, jestliže zajišťují účinnost práva na opravný prostředek?“

Věc C-512/18

- 69 Podáním ze dne 1. září 2015 předložily French Data Network, La Quadrature du Net a Fédération des fournisseurs d'accès à Internet associatifs ke Conseil d'État (Státní rada) návrh na zrušení implicitního zamítavého rozhodnutí, za které lze považovat skutečnost, že Premier ministre (předseda vlády) nerozhodl o jejich návrhu na zrušení článku R. 10-13 CPCE a nařízení vlády č. 2011-219, odůvodněném zejména tím, že tyto předpisy jsou v rozporu s čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 Listiny. Privacy International a Center for Democracy and Technology bylo povoleno vedlejší účastenství ve sporu v původním řízení.
- 70 V souvislosti s článkem R. 10-13 CPCE a v něm stanovenou povinností plošného a nerozlišujícího uchovávání údajů o komunikaci poukazuje předkládající soud, jehož úvahy se ubírají podobným směrem jako úvahy uvedené ve věci C-511/18, na to, že takové uchovávání umožňuje justičnímu orgánu přístup k údajům o komunikaci uskutečněné jednotlivcem před tím, než se stal podezřelým ze spáchání trestného činu, tudíž toto uchovávání představuje s ničím nesrovnatelný přínos pro vyšetřování, odhalování a stíhání trestných činů.
- 71 Co se týče nařízení vlády č. 2011-219, předkládající soud má za to, že čl. 6 odst. II LCEN, který ukládá povinnost držet a uchovávat pouze údaje týkající se vytváření obsahu, nespadá do oblasti působnosti směrnice 2002/58, jelikož ta je podle jejího čl. 3 odst. 1 omezena na poskytování služeb elektronických komunikací přístupných veřejnosti prostřednictvím veřejných komunikačních sítí v Unii, nýbrž do působnosti směrnice 2000/31.
- 72 Tento soud má nicméně za to, že z čl. 15 odst. 1 a 2 směrnice 2000/31 vyplývá, že tato směrnice nezavádí zásadní zákaz uchovávání údajů týkajících se vytváření obsahu, od něhož by bylo možné se odchýlit pouze výjimečně. Vystává tak otázka, zda články 12, 14 a 15 uvedené směrnice, nahlížené ve světle článků 6 až 8 a 11 a čl. 52 odst. 1 Listiny, musí být vykládány v tom smyslu, že umožňují členskému státu zavést takovou vnitrostátní právní úpravu, jako je čl. 6 odst. II LCEN, která ukládá dotčeným osobám uchovávat údaje umožňující identifikaci kohokoli, kdo se podílel na vytváření obsahu nebo části obsahu služeb, které poskytují, aby mohl justiční orgán v případě potřeby požadovat informace s cílem zajistit dodržování pravidel týkajících se občanskoprávní nebo trestněprávní odpovědnosti.
- 73 Za těchto podmínek se Conseil d'État (Státní rada) rozhodla přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:
- „1) Je třeba na povinnost plošného a nerozlišujícího uchovávání uloženou poskytovatelům na základě ustanovení čl. 15 odst. 1 směrnice [2002/58] nahlížet zejména s ohledem na záruky a kontroly, se kterými je následně spojeno shromažďování a využívání údajů o připojení, tak, že jde o zásah odůvodněný právem na bezpečnost, které je zaručeno článkem 6 [Listiny], a požadavky národní bezpečnosti, za které podle článku 4 [SEU] nesou odpovědnost výhradně členské státy?
- 2) Musí být ustanovení směrnice [2000/31] nahlížena ve světle článků 6, 7, 8 a 11 a čl. 52 odst. 1 [Listiny] vykládána v tom smyslu, že umožňují státu přijmout vnitrostátní právní úpravu ukládající osobám, jejichž činností je poskytování přístupu k veřejným komunikačním službám on-line, a fyzickým či právníkům osobám, které i bezúplatně nabízejí veřejnosti veřejné komunikační služby on-line, ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb, povinnost uchovávat údaje, na jejichž základě lze zjistit totožnost kohokoli, kdo přispěl k vytváření obsahu nebo části obsahu služeb, které tyto osoby poskytují, aby mohl justiční orgán v případě potřeby požadovat informace s cílem zajistit dodržování pravidel týkajících se občanskoprávní nebo trestněprávní odpovědnosti?“

Věc C-520/18

- 74 Podáními ze dne 10. ledna, 16. ledna, 17. ledna a 18. ledna 2017, která byla v rámci původního řízení spojena, předložily Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL a UA, Liga voor Mensenrechten ASBL a Ligue des droits de l'Homme ASBL, jakož i VZ, WY a XX ke Cour constitutionnelle (Ústavní soud, Belgie) ústavní stížnosti směřující ke zrušení zákona ze dne 29. května 2016, a to z důvodu, že tento zákon je v rozporu s články 10 a 11 belgické Ústavy ve spojení s články 5, 6 až 11, 14, 15, 17 a 18 EÚLP, s články 7, 8, 11, 47 a čl. 52 odst. 1 Listiny, s článkem 17 Mezinárodního paktu o občanských a politických právech, přijatého Valným shromážděním Organizace spojených národů dne 16. prosince 1966, který vstoupil v platnost dne 23. března 1976, s obecnými zásadami právní jistoty, proporcionality a informačního sebeurčení, jakož i s čl. 5 odst. 4 SEU.
- 75 Stěžovatelé v původním řízení na podporu svých stížností v podstatě tvrdí, že protiprávnost zákona ze dne 29. května 2016 spočívá zejména ve skutečnosti, že zákon překračuje meze toho, co je naprosto nezbytné, a nestanoví dostatečné záruky ochrany. Konkrétně ustanovení týkající se uchovávání údajů ani ustanovení upravující přístup orgánů k uchovávaným údajům neodpovídají požadavkům vyplývajícím z rozsudku ze dne 8. dubna 2014, Digital Rights Ireland a další (C-293/12 a C-594/12, dále jen „rozsudek Digital Rights“, EU:C:2014:238), a z rozsudku ze dne 21. prosince 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970). Tato ustanovení totiž obsahují riziko, že budou vytvářeny osobnostní profily s možností zneužití ze strany příslušných orgánů, která z toho vyplývá, přičemž zároveň nestanoví přiměřenou úroveň zabezpečení a ochrany uchovávaných údajů. Konečně se tento zákon vztahuje i na osoby podléhající profesnímu tajemství a osoby, které mají povinnost zachovávat mlčenlivost, a týká se citlivých komunikačních údajů osobní povahy, přičemž neobsahuje zvláštní záruky na ochranu posledně uvedených údajů.
- 76 Předkládající soud uvádí, že údaje, které musí podle zákona ze dne 29. května 2016 uchovávat poskytovatelé telefonních služeb, včetně internetové telefonie, přístupu k internetu a elektronické pošty, jakož i provozovatelé zajišťující veřejné sítě elektronických komunikací, jsou totožné s údaji uvedenými ve směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (Úř. věst. 2006, L 105, s. 54), přičemž se nerozlišuje mezi dotčenými osobami nebo podle sledovaného cíle. V posledně uvedeném ohledu tento soud upřesňuje, že cílem sledovaným zákonodárcem prostřednictvím tohoto zákona není pouze boj proti terorismu a dětské pornografii, ale rovněž možnost používat uchovávané údaje v široké škále situací v rámci trestního vyšetřování. Předkládající soud mimoto konstatuje, že z důvodové zprávy k uvedenému zákonu vyplývá, že vnitrostátní zákonodárce měl za to, že s ohledem na sledovaný cíl nelze zavést cílenou a diferencovanou povinnost uchovávat údaje a že se rozhodl spojit povinnost plošného a nerozlišujícího uchovávání s přísnými zárukami z hlediska jak uchovávaných údajů, tak přístupu k nim, aby byl zásah do práva na respektování soukromého života omezen na minimum.
- 77 Předkládající soud dodává, že čl. 126 odst. 2 body 1 a 2 zákona ze dne 13. června 2005, ve znění zákona ze dne 29. května 2016, stanoví podmínky, za kterých mohou justiční orgány a zpravodajské a bezpečnostní služby získat přístup k uchovávaným údajům, a tudíž přezkum legality tohoto zákona vzhledem k požadavkům unijního práva musí být přerušen do doby, než Soudní dvůr vydá svá rozhodnutí ve dvou řízeních o předběžné otázce, která před ním probíhají a týkají se takového přístupu.
- 78 Konečně předkládající soud uvádí, že zákon ze dne 29. května 2016 má za cíl umožnit účinné trestní vyšetřování a účinné sankce v případě pohlavního zneužívání nezletilých, jakož i umožnit identifikaci pachatele takového trestného činu, i když jsou používány prostředky elektronické komunikace. V řízeních před předkládajícím soudem byla v tomto ohledu věnována pozornost pozitivním

povinnostem vyplývajícím z článků 3 a 8 EÚLP. Tyto povinnosti by mohly vyplývat rovněž z odpovídajících ustanovení Listiny, jež by mohly mít dopad na výklad čl. 15 odst. 1 směrnice 2002/58.

79 Za těchto okolností se Cour constitutionnelle (Ústavní soud) rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

- „1) Musí být čl. 15 odst. 1 směrnice [2002/58] ve spojení s právem na bezpečnost zaručeným v článku 6 [Listiny] a právem na ochranu osobních údajů, jak je zaručeno články 7 a 8 a článkem 52 [odst. 1] [Listiny], vykládán v tom smyslu, že brání takové vnitrostátní právní úpravě, jako je dotčená právní úprava, jež stanoví plošnou povinnost provozovatelů a poskytovatelů služeb elektronických komunikací uchovávat provozní a lokalizační údaje ve smyslu směrnice [2002/58], které jsou jimi vytvářeny nebo zpracovávány při poskytování těchto služeb, přičemž cílem této vnitrostátní právní úpravy není pouze vyšetřování, odhalování a stíhání závažných trestných činů, ale také zajištění národní bezpečnosti, obrany území a veřejné bezpečnosti, vyšetřování, odhalování a stíhání jiných než závažných trestných činů či předcházení zakázanému použití systémů elektronických komunikací, anebo dosažení jiného cíle uvedeného v čl. 23 odst. 1 nařízení [2016/679], a která kromě toho podléhá zárukám stanoveným v této právní úpravě ohledně uchovávání údajů a přístupu k nim?
- 2) Musí být čl. 15 odst. 1 směrnice [2002/58] ve spojení s články 4, 7, 8 a 11 a čl. 52 odst. 1 [Listiny] vykládán v tom smyslu, že brání takové vnitrostátní právní úpravě, jako je dotčená právní úprava, jež stanoví plošnou povinnost provozovatelů a poskytovatelů služeb elektronických komunikací uchovávat provozní a lokalizační údaje ve smyslu směrnice [2002/58], které jsou jimi vytvářeny nebo zpracovávány při poskytování těchto služeb, pokud je cílem této právní úpravy mimo jiné splnit pozitivní povinnosti orgánů na základě článků 4 a [7] Listiny spočívající ve stanovení právního rámce, který umožňuje vést účinné trestní vyšetřování a stanovit účinný postih sexuálního zneužívání mladistvých a umožňuje skutečně identifikovat pachatele činu, i když jsou používány prostředky elektronické komunikace?
- 3) V případě, že by měl Cour constitutionnelle [(Ústavní soud)] na základě odpovědí poskytnutých na první nebo druhou předběžnou otázku dospět k závěru, že je napadený zákon v rozporu s jednou či více povinnostmi vyplývajících z ustanovení uvedených v těchto otázkách, mohl by dočasně zachovat účinky zákona [ze dne 29. května 2016], aby bylo zabráněno právní nejistotě a aby mohly být předtím shromážděné a uchované údaje dále využívány pro účely stanovené zákonem?“

K řízení před Soudním dvorem

80 Rozhodnutím předsedy Soudního dvora ze dne 25. září 2018 byly věci C-511/18 a C-512/18 spojeny pro účely písemné a ústní části řízení, jakož i pro účely rozsudku. Věc C-520/18 byla spojena s těmito věcmi rozhodnutím předsedy Soudního dvora ze dne 9. července 2020 pro účely rozsudku.

K předběžným otázkám

K prvním otázkám ve věcech C-511/18 a C-512/18, jakož i k první a druhé otázce ve věci C-520/18

81 Podstatou prvních otázek předkládajícího soudu ve věcech C-511/18 a C-512/18, jakož i první a druhé otázky ve věci C-520/18, které je třeba zkoumat společně, je, zda musí být čl. 15 odst. 1 směrnice 2002/58 vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která poskytovatelům služeb elektronických komunikací ukládá pro účely stanovené v tomto čl. 15 odst. 1 povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů.

Úvodní poznámky

- 82 Ze spisů, které má Soudní dvůr k dispozici, vyplývá, že právní úpravy dotčené ve věcech v původních řízeních se vztahují na všechny prostředky elektronické komunikace a zahrnují všechny uživatele těchto prostředků, aniž jsou v tomto ohledu činěny rozdíly nebo výjimky. Kromě toho údaj, který mají podle těchto právních předpisů poskytovatelé služeb elektronických komunikací uchovávat, jsou zejména ty, které jsou nezbytné k nalezení zdroje komunikace a jejího určení, určení dne, hodiny, doby trvání a typu komunikace, určení použitého komunikačního zařízení, jakož i umístění koncových zařízení a komunikací, a mezi něž patří zejména jméno a adresa uživatele, telefonní čísla volajícího a volaného, jakož i adresa IP u internetových služeb. Naproti tomu uvedené údaje nezahrnují obsah dotčených komunikací.
- 83 Údaje, které musí být podle vnitrostátních právních předpisů dotčených ve věcech v původních řízeních uchovávány po dobu jednoho roku, tak umožňují zejména zjistit, se kterou osobou uživatel prostředku elektronické komunikace komunikoval a jaký prostředek byl k této komunikaci použit, určit datum, čas a dobu trvání komunikací a připojení k internetu, jakož i místo, ze kterého probíhaly, a znát umístění koncových zařízení, aniž nutně musí docházet k přenosu sdělení. Dále nabízejí možnost určit četnost komunikací uživatele s určitými osobami v průběhu daného období. Konečně, pokud jde o vnitrostátní právní úpravu dotčenou ve věcech C-511/18 a C-512/18, tato právní úprava vzhledem k tomu, že se vztahuje též na údaje týkající se přenosu elektronických komunikací sítěmi, podle všeho umožňuje rovněž identifikovat povahu informací, které jsou vyhledávány on-line.
- 84 Ke sledovaným cílům je třeba uvést, že právní úpravy dotčené ve věcech C-511/18 a C-512/18 se mimo jiné týkají vyšetřování, odhalování a stíhání trestných činů obecně, národní nezávislosti, územní celistvosti a národní obrany, zásadních zájmů zahraniční politiky, plnění evropských a mezinárodních závazků Francie, významných hospodářských, průmyslových a vědeckých zájmů, jakož i předcházení terorismu, zásahům do republikánského uspořádání orgánů a kolektivnímu násilí, které může závažně narušit veřejný pořádek. Cílem právní úpravy dotčené ve věci C-520/18 je mimo jiné vyšetřování, odhalování a stíhání trestných činů, jakož i zajištění národní bezpečnosti, obrany území a veřejné bezpečnosti.
- 85 Předkládající soudy si kladou zejména otázku týkající se případných dopadů práva na bezpečnost zakotveného v článku 6 Listiny pro výklad čl. 15 odst. 1 směrnice 2002/58. Stejně tak si kladou otázku, zda lze zásah do základních práv zakotvených v člancích 7 a 8 Listiny, představovaný uchováváním údajů podle právních předpisů dotčených ve věcech v původních řízeních, považovat s ohledem na existenci pravidel omezujících přístup vnitrostátních orgánů k uchovávaným údajům za odůvodněný. Dále vzhledem k tomu, že podle Conseil d'État (Státní rada) tato otázka vyvstala za okolností vyznačujících se vážným a trvajícím ohrožením národní bezpečnosti, musí být rovněž posouzena vzhledem k čl. 4 odst. 2 SEU. Cour constitutionnelle (Ústavní soud) zdůrazňuje, že vnitrostátní právní úprava dotčená ve věci C-520/18 rovněž provádí pozitivní povinnosti vyplývající z článků 4 a 7 Listiny, které spočívají ve stanovení právního rámce umožňujícího účinné potírání sexuálního zneužívání nezletilých.
- 86 Zatímco Conseil d'État (Státní rada) i Cour constitutionnelle (Ústavní soud) vycházejí z předpokladu, že vnitrostátní právní úpravy dotčené ve věcech v původních řízeních, které upravují uchovávání provozních a lokalizačních údajů, jakož i přístup k těmto údajům ze strany vnitrostátních orgánů pro účely stanovené v čl. 15 odst. 1 směrnice 2002/58, jako je zajištění národní bezpečnosti, spadají do oblasti působnosti této směrnice, někteří účastníci původních řízení a některé z členských států, které předložily Soudnímu dvoru písemná vyjádření, vyjadřují v tomto ohledu odlišné stanovisko, zejména k výkladu čl. 1 odst. 3 uvedené směrnice. Je tedy třeba nejprve zkoumat, zda uvedené právní úpravy spadají do oblasti působnosti této směrnice.

K oblasti působnosti směrnice 2002/58

- 87 La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International a Center for Democracy and Technology v podstatě uvádějí, přičemž se v tomto ohledu odvolávají na judikaturu Soudního dvora k oblasti působnosti směrnice 2002/58, že uchovávání údajů i přístup k uchovávaným údajům spadají do této působnosti bez ohledu na to, zda k tomuto přístupu dochází až následně, nebo v reálném čase. Vzhledem k tomu, že cíl zajištění národní bezpečnosti je výslovně uveden v čl. 15 odst. 1 této směrnice, nevede sledování tohoto cíle k nepoužitelnosti uvedené směrnice. Článek 4 odst. 2 SEU, na který odkazují předkládající soudy, nemá na tento závěr vliv.
- 88 Ke zpravodajským opatřením, která příslušné francouzské orgány provádějí přímo, aniž upravují činnost poskytovatelů služeb elektronických komunikací uložením zvláštních povinností, Center for Democracy and Technology poznamenává, že tato opatření nutně spadají do oblasti působnosti směrnice 2002/58 a Listiny, jelikož představují výjimky ze zásady důvěrnosti zaručené v článku 5 této směrnice. Uvedená opatření tedy musí splňovat požadavky vyplývající z čl. 15 odst. 1 této směrnice.
- 89 Naproti tomu francouzská, česká a estonská vláda, Irsko, kyperská, maďarská, polská a švédská vláda a vláda Spojeného království v podstatě tvrdí, že směrnice 2002/58 se na takové vnitrostátní právní úpravy, jako jsou úpravy dotčené ve věcech v původních řízeních, nevztahuje, protože účelem těchto právních úprav je zajištění národní bezpečnosti. Činnosti 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.
- 90 Tyto vlády a Irsko navíc odkazují na čl. 1 odst. 3 směrnice 2002/58, který z oblasti působnosti této směrnice vylučuje – stejně jako stanovil již dříve čl. 3 odst. 2 první odrážka směrnice 95/46 – činnosti týkající se veřejné bezpečnosti, obrany a bezpečnosti státu. V tomto ohledu se opírají o výklad posledně uvedeného ustanovení v rozsudku ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346).
- 91 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.
- 92 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 a bezpečnosti státu, včetně 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).
- 93 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 směrnicí 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).
- 94 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. června 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 71).

- 95 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).
- 96 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).
- 97 S ohledem na úvahy uvedené výše v bodě 95 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 svého 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).
- 98 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), vykládat v tom smyslu, že zahrnuje i legislativní opatření uvedená v čl. 15 odst. 1 této směrnice.
- 99 Ustanovení čl. 4 odst. 2 SEU, kterých se dovolávají vlády zmíněné výše v bodě 89 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; ze dne 20. března 2018, *Komise v. Rakousko* (Státní tiskárna), C-187/16, EU:C:2018:194, body 75 a 76, a ze dne 2. dubna 2020, *Komise v. Polsko, Maďarsko a Česká republika* (Dočasný mechanismus relokační žadatelů o mezinárodní ochranu), C-715/17, C-718/17 a C-719/17, EU:C:2020:257, body 143 a 170].
- 100 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.
- 101 Tuto judikaturu ovšem nelze – s ohledem na úvahy uvedené v bodech 93, 95, a 96 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 94 až 97 tohoto rozsudku, do oblasti působnosti uvedené směrnice spadá veškeré zpracování 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.

- 102 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 popsany 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.
- 103 Naproti tomu v případech, kdy členské státy přímo provádějí opatření odchylovající 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.
- 104 Z výše uvedených úvah vyplývá, že vnitrostátní právní úprava, která poskytovatelům služeb elektronických komunikací ukládá povinnost uchovávat takové provozní a lokalizační údaje za účelem zajištění národní bezpečnosti a boje proti trestné činnosti, jako jsou údaje dotčené ve věcech v původních řízeních, spadá do oblasti působnosti směrnice 2002/58.

K výkladu čl. 15 odst. 1 směrnice 2002/58

- 105 Úvodem je třeba připomenout, že podle ustálené judikatury je třeba pro výklad ustanovení unijního práva zohlednit nejen jeho znění, ale i jeho kontext a cíle sledované právní úpravou, jehož je součástí, a zejména genezi této právní úpravy (v tomto smyslu viz rozsudek ze dne 17. dubna 2018, Egenberger, C-414/16, EU:C:2018:257, bod 44).
- 106 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 ze 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“.

- 107 Za tímto účelem zakotvuje čl. 5 odst. 1 směrnice 2002/58 zásadu 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.
- 108 Co se týče konkrétně zpracovávání a uchovávání provozních údajů poskytovateli služeb elektronických komunikací, z článku 6, jakož i z bodů 22 a 26 odůvodnění směrnice 2002/58, vyplývá, že takové zpracování je povoleno pouze v rozsahu a na dobu, jež jsou nezbytné pro účely marketingu těchto služeb, účtování a poskytování služeb s přidanou hodnotou. Po uplynutí této doby musí být zpracováváné a uchovávané údaje vymazány nebo anonymizovány. V případě lokalizačních údajů odlišných od provozních údajů se v čl. 9 odst. 1 uvedené směrnice stanoví, že tyto údaje lze zpracovávat pouze tehdy, jsou-li splněny určité podmínky, a poté, co byly anonymizovány, anebo se souhlasem uživatelů nebo účastníků (rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 86 a citovaná judikatura).
- 109 Přijetím této směrnice tedy unijní normotvůrce konkretizoval práva zakotvená v člancích 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.
- 110 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 povinnosti sice zaručit důvěrnost osobních údajů, a z navazujících povinností stanovených zejména v člancích 6 a 9 uvedené směrnice, pokud takové omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti, obrany a 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.
- 111 Možností odchýlit se od práv a povinností stanovených v člancích 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 rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 89 a 104).
- 112 Pokud jde o cíle, které mohou ospravedlňovat omezení práv a povinností stanovených zejména v člancích 5, 6 a 9 směrnice 2002/58, Soudní dvůr již rozhodl, že výčet cílů v čl. 15 odst. 1 první větě této směrnice je taxativní, a proto musí legislativní opatření přijaté na základě tohoto ustanovení skutečně a nezbytně odpovídat některému z těchto cílů (v tomto smyslu viz rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 52 a citovaná judikatura).
- 113 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 člancích 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 a 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 a 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, C-293/12 a C-594/12, EU:C:2014:238, body 25 a 70, a ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 91 a 92 a citovaná judikatura).

- 114 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).
- 115 V tomto ohledu je třeba upřesnit, že uchovávání provozních a lokalizačních údajů představuje samo o sobě jednak výjimku ze zákazu uloženého jakékoli jiné osobě než uživatelům uchovávat tyto údaje, který je stanoven v čl. 5 odst. 1 směrnice 2002/58, a jednak zásah do základních práv na respektování soukromého života a na ochranu osobních údajů zakotvených v článcích 7 a 8 Listiny bez ohledu na to, 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; obdobně, pokud jde o článek 8 EÚLP, viz rozsudek ESLP ze dne 30. ledna 2020, *Breyer v. Německo*, CE:ECHR:2020:0130JUD005000112, bod 81].
- 116 Není ani rozhodné, zda uchovávané údaje jsou či nejsou následně využity (obdobně, pokud jde o článek 8 EÚLP, viz rozsudky ESLP ze dne 16. února 2000, *Amann v. Švýcarsko*, CE:ECHR:2000:0216JUD002779895, bod 69, a ze dne 13. února 2020, *Trjakovski a Chipovski v. Severní Makedonie* CE:ECHR:2020:0213JUD005320513, bod 51), jelikož přístup k takovým údajům představuje bez ohledu na jejich následné využití odlišný zásah do základních práv uvedených v předchozím bodě [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].
- 117 Tento závěr se jeví o to více důvodný, že provozní a lokalizační údaje mohou odhalit informace o celé řadě aspektů soukromého života subjektů údajů včetně citlivých informací, jako jsou sexuální orientace, politické názory, náboženské, filozofické, sociálněprávní nebo jiné přesvědčení, jakož i zdravotní stav, přičemž takové údaje kromě toho požívají zvláštní ochrany v unijním právu. Z těchto údajů jako celku lze vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovány, tedy o každodenních zvyklostech, o místech, kde trvale či přechodně pobývají, o denních či jiných přesunech, o aktivitách, společenských vztazích těchto osob a o společenských kruzích, s kterými se stýkají. Na základě těchto údajů lze zejména vytvořit profil subjektů údajů, který je s ohledem na právo na ochranu soukromého života informací stejně citlivé povahy, jako je samotný obsah sdělení (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, *Digital Rights*, C-293/12 a C-594/12, EU:C:2014:238, bod 27, a ze dne 21. prosince 2016, *Tele2*, C-203/15 a C-698/15, EU:C:2016:970, bod 99).
- 118 Uchovávání provozních a lokalizačních údajů pro policejní účely tedy, na jedné straně, 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 (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, *Digital Rights*, C-293/12 a C-594/12, EU:C:2014:238, bod 28, a ze dne 21. prosince 2016, *Tele2*, C-203/15 a C-698/15, EU:C:2016:970, bod 101). 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 uchovávaných údajů.

- 119 Na druhé straně s ohledem na značné množství provozních a lokalizačních údajů, které mohou být průběžně uchovávány na základě plošného a nerozlišujícího opatření, a na citlivou povahu informací, které z těchto údajů mohou vyplynout, vzniká riziko zneužití a neoprávněného přístupu již samotným uchováváním těchto údajů poskytovateli služeb elektronických komunikací.
- 120 Článek 15 odst. 1 směrnice 2002/58 ovšem tím, že umožňuje členským státům zavést výjimky uvedené v bodě 110 tohoto rozsudku, odráží tu skutečnost, že se práva zakotvená v článcích 7, 8 a 11 Listiny se 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).
- 121 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.
- 122 Výklad čl. 15 odst. 1 směrnice 2002/58 ve světle Listiny proto vyžaduje, aby byl zohledněn rovněž význam práv zakotvených v článcích 3, 4, 6 a 7 Listiny a význam, který představují cíle zajištění národní bezpečnosti a boje proti závažné trestné činnosti tím, že přispívají k ochraně práv a svobod jiných.
- 123 V tomto ohledu článek 6 Listiny, na který odkazují Conseil d'État (Státní rada) a Cour constitutionnelle (Ústavní soud), zakotvuje právo každého nejen na svobodu, ale i na osobní bezpečnost, a zaručuje práva odpovídající právům zakotveným v článku 5 EÚLP (v tomto smyslu viz rozsudky ze dne 15. února 2016, N., C-601/15 PPU, EU:C:2016:84, bod 47; ze dne 28. července 2016, JZ, C-294/16 PPU, EU:C:2016:610, bod 48, a ze dne 19. září 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, bod 42 a citovaná judikatura).
- 124 Kromě toho je třeba připomenout, že cílem čl. 52 odst. 3 Listiny je zajistit nezbytný soulad mezi právy obsaženými v Listině a odpovídajícími právy zaručenými EÚLP, aniž je narušena autonomie unijního práva a Soudního dvora Evropské unie. Pro účely výkladu Listiny je tedy třeba zohlednit odpovídající práva EÚLP jakožto minimální úroveň ochrany [v tomto smyslu viz rozsudky ze dne 12. února 2019, TC, C-492/18 PPU, EU:C:2019:108, bod 57, ze dne 21. května 2019, Komise v. Maďarsko (Poživací práva k zemědělské půdě), C-235/17, EU:C:2019:432, bod 72 a citovaná judikatura].
- 125 Článek 5 EÚLP, který zakotvuje „právo na svobodu“ a „právo na osobní bezpečnost“, má podle judikatury Evropského soudu pro lidská práva chránit jednotlivce před svévolným nebo neodůvodněným zbavením svobody (v tomto smyslu viz rozsudky ESLP ze dne 18. března 2008, Ladent v. Polsko, CE:ECHR:2008:0318JUD001103603, body 45 a 46; ze dne 29. března 2010, Medvedev a další v. Francie, CE:ECHR:2010:0329JUD000339403, body 76 a 77, a ze dne 13. prosince 2012, El-Masri v. „Bývalá jugoslávská republika Makedonie“ CE:ECHR:2012:1213JUD003963009, bod 239). Avšak vzhledem k tomu, že se toto ustanovení týká zbavení svobody, jehož se dopustil orgán veřejné moci, nelze článek 6 Listiny vykládat tak, že orgánům veřejné moci ukládá povinnost přijmout zvláštní opatření k trestání některých trestných činů.
- 126 Naproti tomu, pokud jde o konkrétně o účinný boj proti trestným činům, jejichž obětí jsou zejména nezletilí a jiné zranitelné osoby, o kterém se zmínil Cour constitutionnelle (Ústavní soud), je třeba zdůraznit, že z článku 7 Listiny mohou vyplývat pozitivní povinnosti orgánů veřejné moci za účelem přijetí právních opatření na ochranu soukromého a rodinného života [v tomto viz smyslu rozsudek ze dne 18. června 2020, Komise v. Maďarsko (Transparentnost sdružování), C-78/18, EU:C:2020:476, bod 123 a citovaná judikatura Evropského soudu pro lidská práva]. Takové povinnosti mohou rovněž vyplývat z uvedeného článku 7 v souvislosti s ochranou obydlí a komunikace, jakož i z článku 3 v souvislosti s ochranou fyzické a duševní nedotknutelnosti osob a z článku 4 v souvislosti se zákazem mučení a nelidského či ponižujícího zacházení.

- 127 Vzhledem k těmto jednotlivým pozitivním povinnostem je přitom třeba přistoupit k nezbytnému sladění jednotlivých dotčených zájmů a práv.
- 128 Evropský soud pro lidská práva totiž rozhodl, že pozitivní povinnosti vyplývající z článků 3 a 8 EÚLP, jejichž odpovídající záruky jsou obsaženy v člancích 4 a 7 Listiny, zahrnují zejména přijetí hmotněprávních a procesních ustanovení, jakož i praktických opatření umožňujících účinně bojovat proti trestným činům namířeným proti osobám prostřednictvím účinného vyšetřování a stíhání, přičemž tato povinnost je o to významnější, je-li ohroženo fyzické a morální blaho dítěte. Opatření, která přísluší přijmout příslušným orgánům, však musí plně respektovat zákonné postupy a další záruky, které mohou omezit rozsah pravomocí spojených s trestním vyšetřováním, jakož i ostatní svobody a práva. Podle uvedeného soudu je třeba zejména stanovit právní rámec umožňující sladit jednotlivé zájmy a práva, která mají být chráněna (rozsudek ESLP ze dne 28. října 1998, *Osman v. Spojené království*, CE:ECHR:1998:1028JUD002345294, body 115 a 116; ze dne 4. března 2004, *M. C. v. Bulharsko*, CE:ECHR:2003:1204JUD003927298, bod 151; ze dne 24. června 2004, *Von Hannover v. Německo*, CE:ECHR:2004:0624JUD005932000, body 57 a 58, a ze dne 2. prosince 2008, *K. U. v. Finsko*, CE:ECHR:2008:1202JUD 000287202, body 46, 48 a 49).
- 129 Pokud jde o dodržení zásady proporcionality, čl. 15 odst. 1 první věta směrnice 2002/58 stanoví, že členské státy mohou přijmout opatření odchylovící 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.
- 130 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 [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, bod 76, 77 a 86, a ze dne 8. dubna 2014, *Digital Rights*, 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].
- 131 Z judikatury Soudního dvora konkrétně vyplývá, že možnost členských států odůvodnit omezení práv a povinností stanovených zejména v člancích 5, 6 a 9 směrnice 2002/58 musí být posuzována z hlediska závažnosti zásahu, který takové omezení představuje, a musí být ověřeno, že význam cíle obecného zájmu sledovaného tímto omezením je úměrný závažnosti zásahu (v tomto smyslu viz rozsudek ze dne 2. října 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, bod 55 a citovaná judikatura).
- 132 Za účelem splnění požadavku proporcionality musí právní úprava stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a uložit 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, již tvoří citlivé údaje [v tomto smyslu viz rozsudky ze dne 8. dubna 2014, *Digital Rights*, C-293/12 a C-594/12, EU:C:2014:238, body 54 a 55, 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].

- 133 Právní úprava, která stanoví uchovávání osobních údajů, tudíž musí vždy odpovídat objektivním kritériím, která vymezují vztah mezi údaji, které mají být uchovávány, a sledovaným účelem [v tomto smyslu viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 191 a citovaná judikatura, jakož i rozsudek ze dne 3. října 2019, A a další, C-70/18, EU:C:2019:823, bod 63].

– K legislativním opatřením stanovícím preventivní uchovávání provozních a lokalizačních údajů za účelem zajištění národní bezpečnosti

- 134 Je třeba poznamenat, že cíl zajištění národní bezpečnosti uváděný předkládajícími soudy a vládami, které předložily vyjádření, nebyl dosud Soudním dvorem specificky zkoumán v jeho rozsudcích zabývajících se výkladem směrnice 2002/58.
- 135 V tomto ohledu 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.
- 136 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, ač závažné trestné činnosti, a cíle zajistit veřejnou bezpečnost. 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.
- 137 V takových situacích, jako jsou situace popsané v bodech 135 a 136 tohoto rozsudku, tak čl. 15 odst. 1 směrnice 2002/58, vykládaný ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny, v zásadě nebrání legislativnímu opatření, které opravňuje příslušné orgány k tomu, aby uložily poskytovatelům služeb elektronických komunikací povinnost uchovávat provozní a lokalizační údaje všech uživatelů prostředků elektronické komunikace po omezenou dobu, pokud existují dostatečně konkrétní okolnosti, pro které se lze domnívat, že dotčený členský stát čelí takové závažné hrozbě pro národní bezpečnost, jako je hrozba uvedená v bodech 135 a 136 tohoto rozsudku, a která je skutečná a aktuální či předvídatelná. I když se takové opatření vztahuje bez rozdílu na všechny uživatele prostředků elektronické komunikace, aniž tito mají – ve smyslu judikatury uvedené v bodě 133 tohoto rozsudku – na první pohled vazbu na ohrožení národní bezpečnosti tohoto členského státu, je třeba mít za to, že existence takového ohrožení může sama o sobě tuto vazbu prokázat.
- 138 Příkaz preventivně uchovávat údaje o všech uživatelích prostředků elektronické komunikace však musí být časově omezen na to, co je nezbytně nutné. Ačkoli nelze vyloučit, aby byl příkaz k uchovávání údajů uložený poskytovatelům služeb elektronických komunikací z důvodu trvání takového ohrožení obnoven, nesmí doba platnosti jednotlivých příkazů přesáhnout předvídatelnou dobu. Takové uchovávání údajů musí navíc podléhat omezením a musí být spojeno s přísnými zárukami, které umožní účinně chránit osobní údaje subjektů údajů před rizikem zneužití. Toto uchovávání tak nemůže být systematické.
- 139 S ohledem na závažnost zásahu do základních práv zakotvených v člancích 7 a 8 Listiny, který vyplývá z takového plošného a nerozlišujícího uchovávání údajů, je třeba zajistit, aby jeho využívání bylo skutečně omezeno na takové situace, v nichž existuje závažné ohrožení národní bezpečnosti, jako jsou situace uvedené v bodech 135 a 136 tohoto rozsudku. Za tímto účelem je nezbytné, aby rozhodnutí, kterým se poskytovatelům služeb elektronických komunikací ukládá povinnost provádět takové

uchovávání údajů, mohlo být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, přičemž cílem přezkumu bude ověřit, že nastala některá z těchto situací, jakož i dodržení podmínek a záruk, které musí být stanoveny.

– *K legislativním opatřením stanovícím preventivní uchovávání provozních a lokalizačních údajů pro účely boje proti trestné činnosti a zajištění veřejné bezpečnosti*

- 140 Pokud jde o cíl prevence, vyšetřování, odhalování a stíhání trestných činů, podle zásady proporcionality platí, že takové závažné zásahy do základních práv zakotvených v člancích 7 a 8 Listiny, jako jsou ty, které s sebou nese uchovávání provozních a lokalizačních údajů, mohou být odůvodněny pouze bojem proti závažné trestné činnosti a předcházením závažnému ohrožení veřejné bezpečnosti. Cílem spočívajícím v prevenci, vyšetřování, odhalování a stíhání trestných činů obecně proto mohou být odůvodněny pouze zásahy do uvedených základních práv, které nejsou závažné povahy [v tomto smyslu viz rozsudky ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 102, a ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 56 a 57; posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 149].
- 141 Vnitrostátní právní úprava, která stanoví plošné a nerozlišující uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti, překračuje meze toho, co je naprosto nezbytné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 107).
- 142 Vzhledem k citlivé povaze informací, které mohou z provozních a lokalizačních údajů vyplynout, je totiž důvěrnost těchto údajů zásadní pro právo na respektování soukromého života. S ohledem jednak na odrazující účinky, které může mít uchovávání těchto údajů ve vztahu k výkonu základních práv zakotvených v člancích 7 a 11 Listiny a které jsou zmíněny výše v bodě 118 tohoto rozsudku, a jednak na závažnost zásahu, který takové uchovávání představuje, je v demokratické společnosti třeba, aby toto uchovávání bylo, jak stanoví systém zavedený směrnicí 2002/58, výjimkou, a nikoli pravidlem, a aby tyto údaje nemohly být uchovávány systematicky a průběžně. Tento závěr platí i ve vztahu k cílům boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti, jakož i k významu, který je třeba jim přiznat.
- 143 Soudní dvůr mimoto zdůraznil, že právní úprava upravující plošné a nerozlišující uchovávání provozních a lokalizačních údajů se vztahuje na elektronické komunikace téměř veškerého obyvatelstva bez jakéhokoli rozlišování, omezení či výjimky v závislosti na sledovaném cíli. Taková právní úprava se totiž týká, v rozporu s požadavkem připomenutým v bodě 133 tohoto rozsudku, globálně všech osob, které využívají služeb elektronických komunikací, aniž se však tyto osoby nachází, byť nepřímou, v situaci, která může vést k trestnímu stíhání. Vztahuje se tedy i na osoby, v jejichž případě neexistuje žádný důvod se domnívat, že by jejich chování mohlo, byť nepřímou nebo vzdáleně, souviset se závažnou trestnou činností, a zejména nevyžaduje žádnou souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, body 57 a 58, a ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 105).
- 144 Konkrétně, jak již rozhodl Soudní dvůr, se taková právní úprava neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti závažné trestné činnosti (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, bod 59, a ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 106).

- 145 Ani v důsledku pozitivních povinností členských států, které by případně mohly vyplývat z článků 3, 4 a 7 Listiny a které se, jak bylo uvedeno výše v bodech 126 a 128 tohoto rozsudku, týkají zavedení pravidel umožňujících účinný boj proti trestným činům, přitom nelze odůvodnit tak závažné zásahy – obsažené v právní úpravě stanovící uchovávání provozních a lokalizačních údajů – do základních práv zakotvených v článcích 7 a 8 Listiny, a to ve vztahu k téměř veškerému obyvatelstvu, aniž mají údaje dotčených osob nějakou souvislost, byť nepřímou, se sledovaným cílem.
- 146 Naproti tomu v souladu s tím, co bylo uvedeno v bodech 142 až 144 tohoto rozsudku, a s ohledem na nezbytné sladění dotčených práv a zájmů, mohou cíle boje proti závažné trestné činnosti, předcházení závažného narušení veřejné bezpečnosti a a *fortiori* zajištění národní bezpečnosti – se zřetelem k jejich významu – odůvodnit vzhledem k pozitivním povinnostem připomenutým v předchozím bodě, na které poukázal zejména Cour constitutionnelle (Ústavní soud), zvláště závažný zásah spočívající v cíleném uchovávání provozních a lokalizačních údajů.
- 147 V této souvislosti, jak již rozhodl Soudní dvůr, čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny nebrání tomu, aby členský stát přijal právní úpravu, která preventivně umožňuje cílené uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti a předcházení závažnému narušení veřejné bezpečnosti, jakož i za účelem zajištění národní bezpečnosti, za podmínky, že uchovávání je omezeno na to, co je nezbytně nutné, pokud jde o kategorie údajů, které mají být uchovávány, komunikační prostředky, na něž se toto uchovávání vztahuje, dotčené osoby a dobu trvání uchovávání (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 108).
- 148 Pokud jde o vymezení, jehož předmětem musí být takové opatření spočívající v uchovávání údajů, může být stanoveno zejména v závislosti na kategoriích subjektů údajů, jelikož čl. 15 odst. 1 směrnice 2002/58 nebrání právní úpravě založené na objektivních skutečnostech, na jejichž základě lze vymezit okruh osob, jejichž provozní a lokalizační údaje mohou vykazat minimálně nepřímou souvislost se závažnou trestnou činností nebo určitým způsobem přispívat k boji proti závažné trestné činnosti či k předcházení závažnému ohrožení veřejné bezpečnosti nebo národní bezpečnosti (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 111).
- 149 V tomto ohledu je třeba upřesnit, že takto dotčenými osobami mohou být zejména osoby, které byly předtím v rámci příslušných vnitrostátních postupů a na základě objektivních skutečností identifikovány jako osoby představující hrozbu pro veřejnou bezpečnost nebo národní bezpečnost dotčeného členského státu.
- 150 Vymezení opatření, které upravuje uchovávání provozních a lokalizačních údajů, lze zajistit rovněž prostřednictvím zeměpisného kritéria, jestliže příslušné vnitrostátní orgány mají na základě objektivních a nediskriminačních skutečností za to, že v jedné nebo více z územních oblastí existuje zvýšené riziko přípravy či páčání závažných trestných činů (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 111). Těmito oblastmi mohou být zejména místa vyznačující se vysokým počtem závažných trestných činů, místa zvláště vystavená páčání závažné trestné činnosti, jako například místa nebo infrastruktury pravidelně navštěvované velmi vysokým počtem osob, nebo také strategická místa, jako jsou letiště, nádraží nebo zóny výběru mýtného.
- 151 Aby byl zásah, který představují opatření spočívající v cíleném uchovávání popsaná v bodech 147 až 150 tohoto rozsudku, v souladu se zásadou proporcionality, nesmí doba trvání těchto opatření přesáhnout dobu, která je nezbytně nutná s ohledem na sledovaný cíl, jakož i na okolnosti, které je odůvodňují, aniž je dotčena možnost případného obnovení, trvají-li důvody, ze kterých je takové uchovávání i nadále nezbytné.

– K legislativním opatřením stanovícím preventivní uchovávání IP adres a údajů o totožnosti občanů pro účely boje proti trestné činnosti a zajištění veřejné bezpečnosti

- 152 Je třeba uvést, že IP adresy, třebaže jsou součástí provozních údajů, jsou generovány bez spojitosti s určitým sdělením a slouží především k tomu, aby prostřednictvím poskytovatelů služeb elektronických komunikací byly identifikovány fyzické osoby vlastníci koncové zařízení, z něhož probíhá komunikace po internetu. Pokud jsou tedy v oblasti elektronické pošty a telefonování po internetu uchovávány pouze IP adresy zdroje komunikace, a nikoli adresy jejího adresáta, tyto adresy jako takové neodhalují žádnou informaci o třetích osobách, které byly v kontaktu s osobou, jež je původcem komunikace. Tato kategorie údajů je tedy méně citlivá než ostatní provozní údaje.
- 153 Nicméně vzhledem k tomu, že IP adresy mohou být použity zejména k provedení úplného sledování postupu prohlížení uživatelem internetu, a v důsledku toho i jeho on-line činnosti, umožňují tyto údaje vytvořit jeho podrobný profil. Uchovávání a analýza uvedených IP adres, které takové sledování vyžaduje, tak představují závažné zásahy do základních práv uživatele internetu zakotvených v člancích 7 a 8 Listiny, které mohou mít takové odrazující účinky, jako jsou účinky uvedené v bodě 118 tohoto rozsudku.
- 154 Pro účely nezbytného sladění dotčených práv a zájmů, které vyžaduje judikatura citovaná v bodě 130 tohoto rozsudku, je přitom třeba zohlednit skutečnost, že v případě trestného činu spáchaného on-line může IP adresa představovat jediný vyšetřovací prostředek umožňující identifikovat osobu, které byla tato adresa přidělena v okamžiku spáchání tohoto trestného činu. K tomu se připojuje skutečnost, že uchovávání IP adres poskytovateli služeb elektronických komunikací nad rámec doby, po kterou byly tyto údaje přiděleny, se v zásadě nejeví jako nezbytné pro účely vyúčtování dotčených služeb, takže odhalování trestných činů spáchaných on-line se bez využití legislativního opatření podle čl. 15 odst. 1 směrnice 2002/58 může ukázat jako nemožné, jak uvedlo několik vlád ve svých vyjádřeních předložených Soudnímu dvoru. Tak tomu může být, podle tvrzení těchto vlád, zejména v případě zvláště závažných trestných činů v oblasti dětské pornografie, jako je získávání, šíření, předávání nebo zpřístupňování dětské pornografie na internetu ve smyslu čl. 2 písm. c) směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (Úř. věst. 2011, L 335, s. 1).
- 155 Ačkoli je za těchto podmínek pravda, že legislativní opatření stanovící uchovávání IP adres všech fyzických osob, které jsou vlastníky koncového zařízení, z něhož může být přístup k internetu uskutečňován, se vztahuje na osoby, které nemají na první pohled ve smyslu judikatury citované v bodě 133 tohoto rozsudku žádnou spojitost se sledovanými cíli, a že uživatelé internetu mohou v souladu s tím, co bylo konstatováno v bodě 109 tohoto rozsudku, na základě článků 7 a 8 Listiny právem očekávat, že jejich totožnost v zásadě nebude odhalena, legislativní opatření stanovící plošné a nerozlišující uchovávání samotných IP adres přidělených zdroji připojení se v zásadě nejeví být v rozporu s čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, pokud tato možnost podléhá přísným hmotněprávním i procesním podmínkám, kterými se použití těchto údajů musí řídit.
- 156 S ohledem na závažnost zásahu do základních práv zakotvených v člancích 7 a 8 Listiny, který toto uchovávání představuje, může být tento zásah odůvodněn – stejně jako v případě zajištění národní bezpečnosti – pouze bojem proti závažné trestné činnosti a předcházením závažnému ohrožení veřejné bezpečnosti. Kromě toho doba uchovávání nemůže překročit dobu nezbytně nutnou s ohledem na sledovaný cíl. Konečně musí opatření této povahy stanovit přísné podmínky a záruky pro využívání těchto údajů, zejména prostřednictvím sledování, ve vztahu ke komunikacím a činnostem uskutečňovaným subjekty údajů na internetu.

157 Konečně co se týče údajů o totožnosti uživatelů prostředků elektronické komunikace, tyto údaje samy o sobě neumožňují zjistit datum, čas, dobu trvání ani adresáta uskutečněné komunikace ani místa, kde se tato komunikace uskutečnila, či její četnost s určitými osobami v určitém období, takže vyjma jejich kontaktních údajů, jako jsou adresy, neposkytují žádné informace o daných komunikacích, a tudíž ani o soukromí těchto uživatelů. Zásah, který s sebou nese uchovávání těchto údajů, tak v zásadě nelze považovat za závažný (v tomto smyslu viz rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 59 a 60).

158 Z toho vyplývá, že v souladu s tím, co bylo uvedeno v bodě 140 tohoto rozsudku, mohou legislativní opatření týkající se zpracování těchto údajů jako takových, zejména jejich uchovávání a přístupu k nim pouze za účelem identifikace dotčeného uživatele, být odůvodněna, nemohou-li uvedené údaje být spojeny s informacemi o uskutečněných komunikacích, cílem prevence, vyšetřování, odhalování a stíhání trestných činů obecně, na který odkazuje čl. 15 odst. 1 první věta směrnice 2002/58 (v tomto smyslu viz rozsudek ze dne 2. října 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 62).

159 Za těchto podmínek je s ohledem na nezbytné sladění dotčených práv a zájmů a z důvodů uvedených v bodech 131 a 158 tohoto rozsudku třeba mít za to, že i v případě neexistence spojitosti mezi všemi uživateli prostředků elektronické komunikace a sledovanými cíli nebrání čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny legislativnímu opatření, které bez bližšího časového omezení ukládá poskytovatelům služeb elektronických komunikací povinnost uchovávat za účelem prevence, vyšetřování, odhalování a stíhání trestných činů, jakož i zajištění veřejné bezpečnosti, aniž trestné činy nebo ohrožení či narušení veřejné bezpečnosti musí nutně být závažné, údaje týkající se totožnosti všech uživatelů prostředků elektronické komunikace.

– K legislativním opatřením stanovícím urychlené uchování provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti

160 Pokud jde o provozní a lokalizační údaje zpracovávané a uchovávané poskytovateli služeb elektronických komunikací na základě článků 5, 6 a 9 směrnice 2002/58 nebo na základě legislativních opatření přijatých na základě čl. 15 odst. 1 této směrnice, jak jsou popsána v bodech 134 až 159 tohoto rozsudku, je třeba uvést, že tyto údaje musí po uplynutí zákonem vymezené doby pro jejich zpracování a uchovávání být v souladu s vnitrostátními předpisy, kterými se provádí tato směrnice, v zásadě buď vymazány, nebo anonymizovány.

161 V průběhu tohoto zpracování a uchovávání se však mohou vyskytnout situace, v nichž se ukáže jako nezbytné uchovávat uvedené údaje po uplynutí těchto dob za účelem objasnění závažných trestných činů nebo narušení národní bezpečnosti, a to jak v situaci, kdy již bylo možné tato protiprávní jednání či narušení zjistit, tak v situaci, kdy lze na základě objektivního posouzení všech relevantních okolností jejich existenci důvodně předpokládat.

162 V tomto ohledu je třeba poukázat na to, že Úmluva Rady Evropy o počítačové kriminalitě ze dne 23. listopadu 2001 (Série des traités européens – č. 185), která byla podepsána 27 členskými státy a ratifikována 25 z nich a jejímž cílem je usnadnit boj proti trestným činům spáchaným prostřednictvím počítačových sítí, stanoví v článku 14, že smluvní strany přijmou pro účely specifických trestních vyšetřování nebo řízení určitá opatření ohledně již uchovávaných provozních údajů, jako je urychlené uchování těchto údajů. Konkrétně čl. 16 odst. 1 této úmluvy stanoví, že smluvní strany přijmou taková legislativní opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům přikázat anebo obdobně zajistit urychlené uchování provozních dat, které byly uloženy prostřednictvím počítačového systému, zejména pokud existují důvody pro přesvědčení, že tato počítačová data jsou ohrožena ztrátou nebo pozměněním.

- 163 V takové situaci, jako je situace uvedená v bodě 161 tohoto rozsudku, mohou členské státy s ohledem na nezbytné sladění dotčených práv a zájmů uvedené v bodě 130 tohoto rozsudku stanovit v právních předpisech přijatých na základě čl. 15 odst. 1 směrnice 2002/58 možnost přikázat rozhodnutím příslušného orgánu, které podléhá účinnému soudnímu přezkumu, poskytovatelům služeb elektronických komunikací, aby po určenou dobu prováděli urychlené uchování provozních a lokalizačních údajů, jimiž disponují.
- 164 Vzhledem k tomu, že účel takového urychleného uchování již neodpovídá účelům, pro které byly údaje původně shromážděny a uchovávány, a že každé zpracování údajů musí podle čl. 8 odst. 2 Listiny odpovídat stanoveným účelům, musí členské státy ve svých právních předpisech upřesnit účel, pro který může být urychlené uchování údajů provedeno. S ohledem na závažnost zásahu do základních práv zakotvených v člancích 7 a 8 Listiny, který může takové uchovávání představovat, může být tento zásah odůvodněn pouze bojem proti závažné trestné činnosti a *a fortiori* zajištěním národní bezpečnosti. Kromě toho, aby se zajistilo, že zásah, který představuje opatření tohoto typu, bude omezen na to, co je nezbytně nutné, je třeba, aby se povinnost uchovávat týkala pouze provozních a lokalizačních údajů, které by mohly přispět k objasnění závažného trestného činu nebo narušení národní bezpečnosti. Také doba uchovávání údajů musí být omezena na to, co je nezbytně nutné, avšak může být prodloužena, pokud to okolnosti a cíl sledovaný uvedeným opatřením odůvodňují.
- 165 V tomto ohledu je třeba upřesnit, že takové urychlené uchování nemusí být omezeno na údaje osob, které jsou konkrétně podezřelé ze spáchání trestného činu nebo z narušení národní bezpečnosti. Při zachování rámce vymezeného v čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny a se zřetelem k úvahám uvedeným v bodě 133 tohoto rozsudku může být takové opatření – podle rozhodnutí zákonodárce a při dodržení mezí toho, co je nezbytně nutné – rozšířeno na provozní a lokalizační údaje týkající se jiných osob než těch, které jsou podezřelé z plánování nebo spáchání závažného trestného činu nebo narušení národní bezpečnosti, pokud tyto údaje mohou na základě objektivních a nediskriminačních kritérií přispět k objasnění takového trestného činu nebo takového narušení národní bezpečnosti, jako například údaje o oběti tohoto činu, o jejím sociálním nebo profesním zázemí, anebo o určitých zeměpisných oblastech, jako jsou místa spáchání nebo přípravy dotčeného trestného činu nebo narušení národní bezpečnosti. Navíc přístup příslušných orgánů k takto uchovávaným údajům musí být prováděn v souladu s podmínkami vyplývajícími z judikatury podávající výklad směrnice 2002/58 (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 118 až 121 a citovaná judikatura).
- 166 Dále je třeba dodat, že přístup k provozním a lokalizačním údajům uchovávaným poskytovateli na základě opatření přijatého podle čl. 15 odst. 1 směrnice 2002/58 může být – jak vyplývá zvláště z bodů 115 a 133 tohoto rozsudku – v zásadě odůvodněn pouze cílem obecného zájmu, pro který bylo těmto poskytovatelům toto uchovávání uloženo. Z toho zejména vyplývá, že přístup k takovým údajům za účelem stíhání a trestání běžné trestné činnosti nemůže být v žádném případě poskytnut, pokud jejich uchovávání bylo odůvodněno cílem boje proti závažné trestné činnosti nebo *a fortiori* zajištění národní bezpečnosti. Naproti tomu v souladu se zásadou proporcionality, jak byla upřesněna v bodě 131 tohoto rozsudku, může být přístup k uchovávaným údajům za účelem boje proti závažné trestné činnosti, pokud jsou dodrženy hmotněprávní a procesní podmínky takového přístupu uvedené v předchozím bodě, odůvodněn cílem zajištění národní bezpečnosti.
- 167 V tomto ohledu mohou členské státy ve svých právních předpisech stanovit, že ke zpřístupnění provozních a lokalizačních údajů může při dodržení stejných hmotněprávních a procesních podmínek docházet za účelem boje proti závažné trestné činnosti nebo zajištění národní bezpečnosti, pokud poskytovatel uchovává uvedené údaje způsobem, který je v souladu s články 5, 6 a 9 nebo také s čl. 15 odst. 1 směrnice 2002/58.
- 168 S ohledem na všechny výše uvedené úvahy je třeba na první otázky ve věcech C-511/18 a C-512/18, jakož i na první a druhou otázku ve věci C-520/18 odpovědět, že čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny musí být vykládán v tom smyslu, že brání legislativním

opatření, která pro účely stanovené v čl. 15 odst. 1 preventivně stanoví plošné a nerozlišující uchovávání provozních a lokalizačních údajů. Naproti tomu uvedený čl. 15 odst. 1 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny nebrání legislativním opatřením,

- která za účelem zajištění národní bezpečnosti stanoví možnost přikázat poskytovatelům služeb elektronických komunikací, aby prováděli plošné a nerozlišující uchovávání provozních a lokalizačních údajů v situacích, kdy dotýčný členský stát čelí závažnému ohrožení národní bezpečnosti, které se jeví jako skutečné a aktuální nebo předvídatelné, přičemž rozhodnutí o uložení tohoto příkazu může být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, a cílem tohoto přezkumu bude ověřit, že nastala některá z těchto situací, jakož i dodržení podmínek a záruk, které musí být stanoveny, a tento příkaz může být vydán pouze na dobu nezbytně nutnou, avšak s možností prodloužení, pokud ohrožení přetrvává;
- která za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti stanoví cílené uchovávání provozních a lokalizačních údajů, které je na základě objektivních a nediskriminačních kritérií vymezeno kategoriemi dotčených osob nebo prostřednictvím zeměpisného kritéria, na dobu nezbytně nutnou, avšak s možností prodloužení;
- která za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti stanoví plošné a nerozlišující uchovávání IP adres přidělených zdroji připojení, a to po nezbytně nutnou dobu;
- která za účelem zajištění národní bezpečnosti, boje proti trestné činnosti a veřejné bezpečnosti stanoví plošné a nerozlišující uchovávání údajů o totožnosti uživatelů prostředků elektronické komunikace a
- která za účelem boje proti závažné trestné činnosti a *a fortiori* zajištění národní bezpečnosti stanoví možnost přikázat rozhodnutím příslušného orgánu, které podléhá účinnému soudnímu přezkumu, poskytovatelům služeb elektronických komunikací, aby po určenou dobu prováděli urychlené uchování provozních a lokalizačních údajů, jimiž disponují,

pokud tato opatření pomocí jasných a přesných pravidel zajišťují při uchovávání dotčených údajů dodržení souvisejících hmotněprávních a procesních podmínek a pokud subjekty údajů mají k dispozici účinné záruky proti riziku zneužití.

Ke druhé a třetí otázce ve věci C-511/18

- 169 Podstatou druhé a třetí otázky předkládajícího soudu ve věci C-511/18 je, zda musí být čl. 15 odst. 1 směrnice 2002/58 nahlížený ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která poskytovatelům služeb elektronických komunikací ukládá povinnost zavést na svých sítích opatření umožňující jednak automatizovanou analýzu a shromažďování provozních a lokalizačních údajů v reálném čase, a jednak shromažďování technických údajů o umístění používaných koncových zařízení v reálném čase, aniž stanoví povinnost vyrozumět subjekty údajů o tomto zpracování a shromažďování údajů.
- 170 Předkládající soud upřesňuje, že metody shromažďování informací upravené v člancích L. 851-2 až L. 851-4 CSI neznamenaají pro poskytovatele služeb elektronických komunikací zvláštní požadavek na uchovávání provozních a lokalizačních údajů. Konkrétně k automatizované analýze uvedené v článku L. 851-3 CSI tento soud uvádí, že předmětem tohoto zpracování je odhalit na základě kritérií definovaných za tímto účelem připojení, která by mohla ukazovat na hrozbu terorismu. Ohledně shromažďování v reálném čase uvedeného v článku L. 851-2 CSI tento soud konstatuje, že se týká

pouze jedné či více osob předem identifikovaných jako osoby, jež mohou mít vazbu na hrozbu terorismu. Podle téhož soudu mohou být tyto dvě metody prováděny pouze za účelem předcházení terorismu a týkají se údajů uvedených v člancích L. 851-1 a R. 851-5 CSI.

- 171 Předně je třeba upřesnit, že okolnost, že podle článku L. 851-3 CSI neumožňuje automatizovaná analýza, která je v něm upravena, sama o sobě identifikaci uživatelů, jejichž údaje jsou předmětem této analýzy, nebrání tomu, aby takové údaje byly kvalifikovány jako „osobní údaje“. Vzhledem k tomu, že postup stanovený v odstavci IV téhož článku umožňuje v pozdější fázi identifikaci subjektu či subjektů údajů prostřednictvím údajů, u nichž automatizovaná analýza odhalila, že mohou ukazovat na hrozbu terorismu, jsou totiž na základě těchto údajů identifikovatelné všechny osoby, jejichž údaje jsou předmětem automatizované analýzy. Podle definice osobních údajů obsažené v čl. 4 bodě 1 nařízení 2016/679 jsou přitom osobními údaji informace mimo jiné o identifikovatelné osobě.

K automatizované analýze provozních a lokalizačních údajů

- 172 Z článku L. 851-3 CSI vyplývá, že automatizovaná analýza, kterou upravuje, v podstatě odpovídá filtrování veškerých provozních a lokalizačních údajů uchovávaných poskytovateli služeb elektronických komunikací, které tyto poskytovatelé provádějí na žádost příslušných vnitrostátních orgánů a podle jimi stanovených parametrů. Z toho vyplývá, že u veškerých údajů uživatelů prostředků elektronické komunikace je ověřováno, zda odpovídají těmto parametrům. Je tedy třeba mít za to, že taková automatizovaná analýza vyžaduje, aby dotčení poskytovatelé služeb elektronických komunikací prováděli na účet příslušného orgánu plošné a nerozlišující zpracování, které má podobu použití pomocí automatizovaného postupu ve smyslu čl. 4 bodu 2 nařízení 2016/679 a vztahuje se na všechny provozní a lokalizační údaje všech uživatelů prostředků elektronické komunikace. Toto zpracování je nezávislé na následném shromažďování údajů týkajících se osob identifikovaných na základě automatizované analýzy, tedy na shromažďování dovoleném na základě čl. L. 851-3 odst. IV CSI.
- 173 Vnitrostátní právní úprava, která dovoluje takovou automatizovanou analýzu provozních a lokalizačních údajů, se přitom odchyluje od základní povinnosti stanovené v článku 5 směrnice 2002/58, a sice povinnosti zajistit důvěrný charakter elektronických komunikací a s nimi souvisejících údajů. Taková právní úprava rovněž představuje zásah do základních práv zakotvených v člancích 7 a 8 Listiny bez ohledu na následné využití těchto údajů. Konečně uvedená právní úprava může mít podle judikatury citované v bodě 118 tohoto rozsudku odrazující účinky na výkon svobody projevu zakotvené v článku 11 Listiny.
- 174 Kromě toho zásah vyplývající z takové automatizované analýzy provozních a lokalizačních údajů, jako je analýza dotčená ve věci v původním řízení, se jeví jako zvlášť závažný, jelikož plošné a nerozlišujícím způsobem pokrývá údaje osob používajících prostředky elektronické komunikace. Toto zjištění platí tím spíše, pokud – jak vyplývá z vnitrostátní právní úpravy dotčené ve věci v původním řízení – mohou údaje, které jsou předmětem automatizované analýzy, odhalit povahu informací vyhledávaných on-line. Navíc se taková automatizovaná analýza vztahuje globálně na všechny osoby používající prostředky elektronické komunikace, a tudíž i na osoby, v jejichž případě neexistuje žádný důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset s teroristickou činností.
- 175 Pokud jde o odůvodnění takového zásahu, je třeba upřesnit, že požadavek stanovený v čl. 52 odst. 1 Listiny, 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 (v tomto smyslu viz rozsudek ze dne 16. července 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 175 a citovaná judikatura).

- 176 Kromě toho, aby byl splněn požadavek proporcionality připomenutý v bodech 130 a 131 tohoto rozsudku, podle něhož výjimky z ochrany osobních údajů a její omezení musí být činěny v mezích toho, co je nezbytně nutné, musí vnitrostátní právní úprava přístupu příslušných orgánů k uchovávaným provozním a lokalizačním údajům splňovat požadavky vyplývající z judikatury citované v bodě 132 tohoto rozsudku. Konkrétně se taková právní úprava nemůže omezit na požadavek, aby přístup orgánů k údajům odpovídal cíli 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].
- 177 V tomto ohledu je třeba připomenout, že zvlášť závažný zásah, který představuje plošné a nerozlišující uchovávaní provozních a lokalizačních údajů, jímž se zabývají úvahy rozvedené výše v bodech 134 až 139 tohoto rozsudku, jakož i zvlášť závažný zásah, který představuje jejich automatizovaná analýza, mohou splňovat požadavek přiměřenosti pouze v situacích, kdy členský stát čelí závažnému ohrožení národní bezpečnosti, které se jeví jako skutečné a aktuální nebo předvídatelné, a pod podmínkou, že je toto uchovávaní časově omezeno na nezbytně nutnou dobu.
- 178 V takových situacích, jako jsou situace uvedené v předchozím bodě, lze provedení automatizované analýzy provozních a lokalizačních údajů všech uživatelů prostředků elektronické komunikace po striktně omezenou dobu považovat za odůvodněné vzhledem k požadavkům vyplývajícím z čl. 15 odst. 1 směrnice 2002/58 nahlíženého ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny.
- 179 Zaručení toho, že využití takového opatření se skutečně omezí na to, co je nezbytně nutné k zajištění národní bezpečnosti, zvláště k předcházení terorismu, vyžaduje, jak bylo uvedeno v bodě 139 tohoto rozsudku, aby rozhodnutí povolující automatizovanou analýzu mohlo být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, přičemž cílem přezkumu bude ověřit, že nastala situace, která uvedené opatření odůvodňuje, jakož i dodržení podmínek a záruk, které musí být stanoveny.
- 180 V tomto ohledu je třeba upřesnit, že předem stanovené vzorce a kritéria, na nichž se tento druh zpracování údajů zakládá, musí být jednak konkrétní a spolehlivé, aby umožnily dosáhnout výsledků cílených na jednotlivce, vůči kterým může existovat důvodné podezření ohledně účasti na teroristických trestných činech, a jednak nediskriminační [v tomto smyslu viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 172].
- 181 Kromě toho je třeba připomenout, že jakákoli automatizovaná analýza prováděná na základě vzorců a kritérií založených na předpokladu, že rasový či etnický původ, politické názory, náboženské či filozofické přesvědčení, členství v odborech, zdravotní stav nebo sexuální život osoby mohou být samy o sobě a nezávisle na individuálním chování této osoby relevantní z hlediska předcházení terorismu, by byla v rozporu s právy zaručenými články 7 a 8 Listiny ve spojení s jejím článkem 21. Předem stanovené vzorce a kritéria pro účely automatizované analýzy zaměřené na předcházení teroristickým činnostem, které představují závažnou hrozbu pro národní bezpečnost, tak nemohou být založeny pouze na těchto citlivých údajích [v tomto smyslu viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, bod 165].
- 182 Mimoto vzhledem k tomu, že automatizované analýzy provozních a lokalizačních údajů nutně vykazují určitou míru chybovosti, každý pozitivní výsledek získaný automatizovaným zpracováním musí být podroben individuálnímu přezkumu za pomoci neautomatizovaných prostředků před přijetím individuálního opatření s nepříznivým dopadem na dotčené osoby, jako je následné shromažďování provozních a lokalizačních údajů v reálném čase, a tudíž takové opatření nemůže být založeno v rozhodující míře pouze na výsledku automatizovaného zpracování. Stejně tak k zajištění toho, aby předem stanovené vzorce a kritéria, jejich využívání a používané databáze nebyly v praxi diskriminační a byly omezeny na to, co je nezbytně nutné z hlediska cíle předcházet teroristické činnosti představující závažné ohrožení pro národní bezpečnost, musí být spolehlivost a aktuálnost těchto předem

stanovených vzorců a kritérií, jakož i používaných databází, předmětem pravidelného přezkumu [v tomto smyslu viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, body 173 a 174].

Ke shromažďování provozních a lokalizačních údajů v reálném čase

- 183 Co se týče shromažďování provozních a lokalizačních údajů v reálném čase podle článku L. 851-2 CSI, je třeba poukázat na to, že toto shromažďování může být jednotlivě povoleno, pokud se týká „předem identifikované osoby, u níž lze předpokládat, že může mít vazbu na [teroristickou] hrozbu“. Podle tohoto ustanovení platí, že „[e]xistují-li závažné důvody se domnívat, že jedna nebo více osob, které patří do okolí osoby dotčené povolením, může poskytnout informace s ohledem na účel, který odůvodňuje povolení, může být toto povolení rovněž uděleno jednotlivě ve vztahu ke každé z těchto osob“.
- 184 Údaje, které jsou předmětem opatření této povahy, příslušným vnitrostátním orgánům umožňují, aby během platnosti povolení průběžně a v reálném čase sledovaly kontaktní osoby, se kterými dotčené osoby komunikují, prostředky, které využívají, dobu trvání komunikací, které uskutečňují, jakož i místa jejich pobytu a jejich přesuny. Stejně mohou tyto údaje podle všeho odhalit povahu informací vyhledávaných on-line. Jak vyplývá z bodu 117 tohoto rozsudku, z těchto údajů jako celku lze vyvodit velmi přesné závěry o soukromém životě dotčených osob a vytvořit jejich profil, přičemž taková informace je z hlediska práva na respektování soukromého života stejně citlivá jako samotný obsah komunikací.
- 185 Co se týče shromažďování údajů v reálném čase podle článku L. 851-4 CSI, toto ustanovení umožňuje shromažďovat technické údaje o umístění koncových zařízení a a předávat je v reálném čase útvaru předsedy vlády. Takové údaje patrně umožňují příslušnému útvaru kdykoli během platnosti povolení nepřetržitě a v reálném čase lokalizovat použitá koncová zařízení, jako jsou mobilní telefony.
- 186 Vnitrostátní právní úprava dovolující takové shromažďování v reálném čase se přitom stejně jako právní úprava, která dovoluje automatizovanou analýzu údajů, odchyluje od základní povinnosti stanovené v článku 5 směrnice 2002/58 zajistit důvěrný charakter elektronických sdělení a s nimi souvisejících údajů. Představuje tedy rovněž zásah do základních práv zakotvených v člancích 7 a 8 Listiny a může mít odrazující účinky na výkon svobody projevu zaručené v článku 11 Listiny.
- 187 Je třeba zdůraznit, že zásah, který představuje shromažďování – v reálném čase – údajů umožňujících lokalizovat koncové zařízení, se jeví jako zvláště závažný, jelikož tyto údaje poskytují příslušným vnitrostátním orgánům prostředek přesného a neustálého sledování přesunů uživatelů mobilních telefonů. Vzhledem k tomu, že tyto údaje musí tudíž být považovány za obzvláště citlivé, musí být přístup příslušných orgánů k takovým údajům v reálném čase odlišen od následného přístupu k těmto údajům, protože první z nich je invazivnější, neboť umožňuje téměř dokonalý dohled nad těmito uživateli (obdobně, pokud jde o článek 8 EÚLP, viz rozsudek ESLP ze dne 8. února 2018, Ben Faiza v. Francie, CE:ECHR:2018:0208JUD003144612, bod 74). Intenzita tohoto zásahu je mimoto ještě závažnější, pokud se shromažďování v reálném čase vztahuje rovněž na provozní údaje subjektů údajů.
- 188 Ačkoli cíl předcházení terorismu sledovaný vnitrostátní právní úpravou dotčenou ve věci v původním řízení může s ohledem na svůj význam odůvodnit zásah, který představuje shromažďování provozních a lokalizačních údajů v reálném čase, smí být takové opatření vzhledem ke své obzvláště invazivní povaze prováděno pouze ve vztahu k osobám, u nichž existuje pádný důvod se domnívat, že jsou určitým způsobem zapojeny do teroristických činností. Údaje osob, které do této kategorie nespádají, mohou být zpřístupněny pouze následně, přičemž tento přístup může být podle judikatury Soudního dvora poskytnut pouze ve zvláštních situacích, jako jsou situace, v nichž se jedná o teroristické

činnosti, a pokud existují objektivní skutečnosti umožňující mít za to, že by tyto údaje mohly v konkrétním případě účinně přispět k boji proti terorismu (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).

- 189 Kromě toho rozhodnutí, kterým se povoluje shromažďování provozních a lokalizačních údajů v reálném čase, musí být založeno na objektivních kritériích stanovených vnitrostátními právními předpisy. Zvláště musí tyto právní předpisy v souladu s judikaturou citovanou v bodě 176 tohoto rozsudku vymezit okolnosti a podmínky, za kterých může být takové shromažďování povoleno, a stanovit, jak bylo upřesněno v předchozím bodě, že se může vztahovat jen na osoby, u nichž existuje vazba na cíl prevence terorismu. Mimoto musí rozhodnutí, kterým se povoluje shromažďování provozních a lokalizačních údajů v reálném čase, být založeno na objektivních a nediskriminačních kritériích stanovených ve vnitrostátních právních předpisech. Pro zajištění dodržování těchto podmínek v praxi je zásadní, aby provádění opatření, kterým se povoluje shromažďování v reálném čase, podléhalo předchozímu přezkumu prováděnému soudem nebo nezávislým správním orgánem, přičemž tento soud nebo orgán se musí zejména ujistit, že je takové shromažďování v reálném čase povoleno pouze v mezích toho, co je nezbytně nutné (v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 120). V řádně odůvodněných naléhavých případech musí být přezkum proveden v co nejkratší době.

K vyrozumění subjektů, jejichž údaje byly shromážděny nebo analyzovány

- 190 Je důležité, aby příslušné vnitrostátní orgány provádějící shromažďování provozních a lokalizačních údajů v reálném čase vyrozuměly o této skutečnosti subjekty údajů v rámci použitelných vnitrostátních postupů, a to za předpokladu a od okamžiku, kdy tímto sdělením nebude možné ohrozit úkoly uložené těmito orgánům. Taková informace je totiž fakticky nezbytná k tomu, aby tyto subjekty mohly uplatnit svá práva vyplývající z článků 7 a 8 Listiny a žádat o přístup ke svým osobním údajům, které jsou předmětem těchto opatření, a případně o jejich opravu nebo odstranění, jakož i uplatnit v souladu s čl. 47 prvním pododstavcem Listiny účinný prostředek nápravy před soudem, přičemž toto právo je ostatně výslovně zaručeno článkem 15 odst. 2 směrnice 2002/58 ve spojení s čl. 79 odst. 1 nařízení 2016/679 [v tomto smyslu viz rozsudek ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 121 a citovaná judikatura, a posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, body 219 a 220].
- 191 Co se týče vyrozumění požadovaného v souvislosti s automatizovanou analýzou provozních a lokalizačních údajů, je příslušný vnitrostátní orgán povinen uveřejnit informace obecné povahy týkající se této analýzy, ale nemusí subjekty údajů vyrozumět individuálně. Naproti tomu v případě, kdy údaje odpovídají parametrům specifikovaným v opatření, kterým se povoluje automatizovaná analýza, a kdy tento orgán identifikuje subjekt údajů za účelem hlubší analýzy údajů, které se jej týkají, se individuální vyrozumění tohoto subjektu jeví být nezbytným. Takové vyrozumění však smí být provedeno jen za předpokladu a až od okamžiku, kdy nebude moci ohrozit úkoly uložené uvedenému orgánu [obdobně viz posudek 1/15 (Dohoda PNR mezi EU a Kanadou) ze dne 26. července 2017, EU:C:2017:592, body 222 až 224].
- 192 S ohledem na všechny výše uvedené úvahy je třeba na druhou a třetí otázku ve věci C-511/18 odpovědět, že čl. 15 odst. 1 směrnice 2002/58 nahlížený ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny musí být vykládán v tom smyslu, že nebrání vnitrostátní právní úpravě, která poskytovatelům služeb elektronických komunikací ukládá povinnost provádět jednak automatizovanou analýzu a shromažďování zejména provozních a lokalizačních údajů v reálném čase a jednak shromažďování technických údajů o umístění používaných koncových zařízení v reálném čase, pokud

- je provádění automatizované analýzy omezeno na situace, kdy členský stát čelí závažné hrozbě pro národní bezpečnost, která se jeví jako skutečná a aktuální či předvídatelná, přičemž provádění této analýzy může být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, a cílem takového přezkumu bude ověřit, že nastala situace, která uvedené opatření odůvodňuje, jakož i dodržení podmínek a záruk, které musí být stanoveny, a
- je provádění shromažďování provozních a lokalizačních údajů v reálném čase omezeno na subjekty, u nichž existuje pádný důvod se domnívat, že jsou určitým způsobem zapojeny do teroristických činností, a podléhá předchozímu přezkumu prováděnému soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, aby bylo zajištěno, že takové shromažďování v reálném čase bude povoleno pouze v mezích toho, co je nezbytně nutné. V řádně odůvodněných naléhavých případech musí být přezkum proveden v co nejkratší době.

Ke druhé otázce ve věci C-512/18

- 193 Podstatou druhé otázky předkládajícího soudu ve věci C-512/18 je, zda musí být ustanovení směrnice 2000/31 nahlížena ve světle článků 6 až 8 a 11 a čl. 52 odst. 1 Listiny, vykládána v tom smyslu, že brání vnitrostátní právní úpravě, která poskytovatelům veřejných komunikačních služeb on-line a poskytovatelům hostingových služeb ukládá plošné a nerozlišující uchovávání zejména osobních údajů souvisejících s těmito službami.
- 194 Předkládající soud má za to, že takové služby spadají do působnosti směrnice 2000/31, a nikoli do působnosti směrnice 2002/58, a je toho názoru, že čl. 15 odst. 1 a 2 směrnice 2000/31 ve spojení s jejími články 12 a 14 sám o sobě nezavádí zásadní zákaz uchovávání údajů týkajících se vytváření obsahu, od něhož by bylo možné se odchýlit pouze výjimečně. Tento soud si nicméně klade otázku, zda toto posouzení obstojí s ohledem na nutnost respektovat základní práva zakotvená v člancích 6 až 8 a 11 Listiny.
- 195 Předkládající soud dále upřesňuje, že jeho otázka se týká uchovávání upraveného v článku 6 LCEN, ve spojení s nařízením vlády č. 2011-219. Údaje, které musí dotyční poskytovatelé služeb na tomto základě uchovávat, zahrnují zejména údaje týkající se totožnosti osob, které tyto služby využily, jako jsou jejich příjmení, jména, příslušné poštovní adresy, příslušné adresy elektronické pošty nebo účtu, jejich hesla, a je-li uzavření smlouvy nebo otevření účtu zpoplatněno, druh provedené platby, reference platby, částka, datum a čas transakce.
- 196 Údaje, kterých se týká povinnost uchovávání, zahrnují rovněž identifikátory přidělené účastníkům, identifikátory připojení a identifikátory použitých koncových zařízení, identifikátory přidělené obsahu, data a časy zahájení a ukončení připojení a operací, jakož i typy protokolů použitých pro připojení ke službě a pro přenos obsahu. Přístup k těmto údajům, jejichž doba uchovávání činí jeden rok, může být vyžádán v rámci trestních a občanských soudních řízení s cílem zajistit dodržování pravidel týkajících se občanskoprávní či trestněprávní odpovědnosti, jakož i v rámci opatření upravujících shromažďování informací, na něž se vztahuje článek L. 851-1 CSI.
- 197 V tomto ohledu je třeba poznamenat, že směrnice 2000/31 v souladu se svým čl. 1 odst. 2 sblíží některá vnitrostátní ustanovení platná pro služby informační společnosti uvedené v jejím čl. 2 písm. a).
- 198 Takové služby zajisté zahrnují služby, které jsou poskytovány na dálku prostřednictvím elektronických zařízení pro zpracování a uchovávání dat, na individuální žádost příjemce služeb a zpravidla za úplat, jako jsou služby přístupu k internetu nebo ke komunikační síti, jakož i hostingové služby (v tomto smyslu viz rozsudky ze dne 24. listopadu 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, bod 40; ze

dne 16. února 2012, SABAM, C-360/10, EU:C:2012:85, bod 34; ze dne 15. září 2016, Mc Fadden, C-484/14, EU:C:2016:689, bod 55, a ze dne 7. srpna 2018, SNB-REACT, C-521/17, EU:C:2018:639, bod 42 a citovaná judikatura).

- 199 Článek 1 odst. 5 směrnice 2000/31 nicméně stanoví, že tato směrnice se nevztahuje na otázky týkající se služeb informační společnosti upravené ve směrnici 95/46 a 97/66. V tomto ohledu z bodů 14 a 15 odůvodnění směrnice 2000/31 vyplývá, že ochrana důvěrnosti komunikace a fyzických osob v souvislosti se zpracováním osobních údajů v rámci služeb informační společnosti je upravena pouze směrnicemi 95/46 a 97/66, přičemž druhá z nich v článku 5 zakazuje za účelem ochrany důvěrného charakteru sdělení jakoukoli formu zachycování nebo sledování sdělení.
- 200 Otázky související s ochranou důvěrného charakteru sdělení a osobních údajů proto musí být posouzeny podle směrnice 2002/58, která nahradila směrnicí 97/66, a podle nařízení 2016/679, které nahradilo směrnicí 95/46, přičemž ochrana, kterou má zajistit směrnice 2000/31, nemůže v žádném případě působit újmu požadavkům vyplývajícím ze směrnice 2002/58 a nařízení 2016/679 (v tomto smyslu viz rozsudek ze dne 29. ledna 2008, Promusicae, C-275/06, EU:C:2008:54, bod 57).
- 201 Jak v podstatě uvedl generální advokát v bodě 141 svého stanoviska ve spojených věcech La Quadrature du Net a další (C-511/18 a C-512/18, EU:C:2020:6), povinnost uchovávat osobní údaje související s veřejnými komunikačními službami on-line a s hostingovými službami uložená poskytovatelům těchto služeb vnitrostátní právní úpravou uvedenou v bodě 195 tohoto rozsudku tedy musí být posuzována vzhledem ke směrnici 2002/58, resp. nařízení 2016/679.
- 202 Podle toho, zda poskytování služeb, na které se vztahuje tato vnitrostátní právní úprava, spadá či nespadá do působnosti směrnice 2002/58, se tedy toto poskytování bude řídit buď posledně uvedenou směrnicí, zejména jejím čl. 15 odst. 1 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, nebo nařízením 2016/679, zejména článkem 23 odst. 1 uvedeného nařízení ve spojení s týmiž ustanoveními Listiny.
- 203 V projednávané věci nelze vyloučit, jak uvedla Evropská komise ve svém písemném vyjádření, že některé služby, na které se vztahuje vnitrostátní právní úprava uvedená v bodě 195 tohoto rozsudku, představují služby elektronických komunikací ve smyslu směrnice 2002/58, což přísluší ověřit předkládajícímu soudu.
- 204 V tomto ohledu je třeba uvést, že směrnice 2002/58 se vztahuje na služby elektronických komunikací, které splňují podmínky stanovené v čl. 2 písm. c) směrnice 2002/21, na který odkazuje článek 2 směrnice 2002/58 a podle kterého se službou elektronických komunikací rozumí „služba obvykle poskytovaná za úplat, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové vysílání“. Co se týče služeb informační společnosti uvedených v bodech 197 a 198 tohoto rozsudku, na které se vztahuje směrnice 2000/31, tyto představují služby elektronických komunikací, jelikož spočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací (v tomto smyslu viz rozsudek ze dne 5. června 2019, Skype Communications, C-142/18, EU:C:2019:460, body 47 a 48).
- 205 Internetové služby, na které se patrně vztahuje vnitrostátní právní úprava uvedená v bodě 195 tohoto rozsudku, představují, jak potvrzuje bod 10 odůvodnění směrnice 2002/21, služby elektronických komunikací ve smyslu této směrnice (v tomto smyslu viz rozsudek ze dne 5. června 2019, Skype Communications, C-142/18, EU:C:2019:460, bod 37). Stejně je tomu u internetových e-mailových služeb, u kterých podle všeho není vyloučeno, že spadají rovněž pod tuto vnitrostátní právní úpravu, neboť po technické stránce spočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací (v tomto smyslu viz rozsudek ze dne 13. června 2019, Google, C-193/18, EU:C:2019:498, body 35 a 38).

- 206 Co se týče požadavků vyplývajících z čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny, je třeba odkázat na všechna zjištění a posouzení učiněná v rámci odpovědi na první otázku ve věcech C-511/18 a C-512/18, jakož i na první a druhou otázku ve věci C-520/18.
- 207 Pokud jde o požadavky vyplývající z nařízení 2016/679, je třeba připomenout, že cílem tohoto nařízení je, jak vyplývá z bodu 10 jeho odůvodnění, zajistit soudržnou a vysokou úroveň ochrany fyzických osob v Unii, a za tím účelem zajistit v celé Unii jednotné a soudržné uplatňování pravidel ochrany základních práv a svobod těchto osob v souvislosti se zpracováváním osobních údajů (v tomto smyslu viz rozsudek ze dne 16. července 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 101).
- 208 Za tímto účelem musí každé zpracování osobních údajů – s výhradou výjimek, které připouští článek 23 nařízení 2016/679 – v souladu se zásadami, jimiž se řídí zpracování osobních údajů, jakož i s právy subjektu údajů uvedenými v kapitolách II a III tohoto nařízení. Každé zpracování osobních údajů musí být konkrétně jednak v souladu se zásadami stanovenými v článku 5 uvedeného nařízení, a jednak odpovídat podmínkám zákonnosti zpracování, které jsou vyjmenovány v článku 6 téhož nařízení (obdobně, pokud jde o směrnici 95/46, viz rozsudek ze dne 30. května 2013, Worten, C-342/12, EU:C:2013:355, bod 33 a citovaná judikatura).
- 209 Pokud jde konkrétně o čl. 23 odst. 1 nařízení 2016/679, je třeba poznamenat, že toto ustanovení umožňuje členským státům, podobně jako je stanoveno v čl. 15 odst. 1 směrnice 2002/58, omezit s ohledem na cíle, které stanoví, a prostřednictvím legislativních opatření rozsah povinností a práv v něm uvedených, „jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit“ sledovaný cíl. Každé legislativní opatření přijaté na tomto základě musí konkrétně splňovat zvláštní požadavky stanovené v čl. 23 odst. 2 tohoto nařízení.
- 210 Článek 23 odst. 1 a 2 nařízení 2016/679 tedy nelze vykládat tak, že by mohl členské státy oprávnit k zásahu do respektování soukromého života v rozporu s článkem 7 Listiny, nebo do jiných záruk stanovených v této Listině (obdobně, pokud jde o směrnici 95/46, viz rozsudek ze dne 20. května 2003, Österreichischer Rundfunk a další, C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 91). Konkrétně, podobně jako v případě čl. 15 odst. 1 směrnice 2002/58, může být pravomoc, kterou členským státům přiznává čl. 23 odst. 1 nařízení 2016/679, vykonávána pouze při dodržení požadavku proporcionality, podle kterého výjimky z ochrany osobních údajů a její omezení musí být činěny v mezích toho, co je naprosto nezbytné (obdobně, pokud jde o směrnici 95/46, viz rozsudek ze dne 7. listopadu 2013, IPI, C-473/12, EU:C:2013:715, bod 39 a citovaná judikatura).
- 211 Z toho vyplývá, že zjištění a posouzení učiněná v rámci odpovědi na první otázku ve věcech C-511/18 a C-512/18, jakož i na první a druhou otázku ve věci C-520/18 platí obdobně i pro článek 23 nařízení 2016/679.
- 212 S ohledem na výše uvedené úvahy je třeba na druhou otázku ve věci C-512/18 odpovědět, že směrnice 2000/31 musí být vykládána v tom smyslu, že se nevztahuje na oblast ochrany důvěrnosti komunikace a fyzických osob v souvislosti se zpracováním osobních údajů v rámci služeb informační společnosti, jelikož tato ochrana je upravena – podle okolností – směrnicí 2002/58 nebo nařízením 2016/679. Článek 23 odst. 1 nařízení 2016/679 nahlížený ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která poskytovatelům veřejných komunikačních služeb on-line a poskytovatelům hostingových služeb ukládá povinnost plošného a nerozlišujícího uchovávání údajů, zejména osobních údajů souvisejících s těmito službami.

Ke třetí otázce ve věci C-520/18

- 213 Podstatou třetí otázky předkládajícího soudu ve věci C-520/18 je, zda vnitrostátní soud může uplatnit ustanovení svého vnitrostátního práva opravňující jej k tomu, aby časově omezil účinky prohlášení protiprávnosti, které mu přísluší podle tohoto práva, ve vztahu k vnitrostátním právním předpisům, jež poskytovatelům služeb elektronických komunikací ukládají, mimo jiné za účelem sledování cílů zajištění národní bezpečnosti a boje proti trestné činnosti, povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů, z důvodu jejich neslučitelnosti s čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a s čl. 52 odst. 1 Listiny.
- 214 Zásada přednosti unijního práva zakotvuje nadřazenost unijního práva nad právem členských států. Tato zásada tedy ukládá všem orgánům členských států povinnost zajišťovat plný účinek jednotlivých unijních norem, přičemž právo členských států nemůže narušovat účinek přiznaný těmto jednotlivým normám na území uvedených států [rozsudky ze dne 15. července 1964, Costa, 6/64, EU:C:1964:66, s. 1159 a 1160, a ze dne 19. listopadu 2019, A. K. a další (Nezávislost kárného senátu Nejvyššího soudu), C-585/18, C-624/18 a C-625/18, EU:C:2019:982, body 157 a 158 a citovaná judikatura].
- 215 Ze zásady přednosti plyne, že pokud vnitrostátní soud, jež má v rámci svých pravomocí uplatnit ustanovení unijního práva, nemůže vyložit vnitrostátní právní úpravu v souladu s požadavky tohoto práva, má povinnost zajistit plný účinek těchto ustanovení tak, že na základě své vlastní pravomoci podle potřeby upustí od použití jakéhokoli odporujícího ustanovení vnitrostátních právních předpisů, i když je pozdějšího data, aniž musí nejprve žádat o jeho odstranění legislativní cestou nebo jakýmkoliv jiným ústavním postupem či na toto odstranění čekat [rozsudky ze dne 22. června 2010, Melki a Abdeli, C-188/10 a C-189/10, EU:C:2010:363, bod 43 a citovaná judikatura; ze dne 24. června 2019, Popławski, C-573/17, EU:C:2019:530, bod 58, a ze dne 19. listopadu 2019, A. K. a další (Nezávislost kárného kolegia Nejvyššího soudu), C-585/18, C-624/18 a C-625/18, EU:C:2019:982, bod 160].
- 216 Jedině Soudní dvůr může výjimečně a z naléhavých důvodů právní jistoty přiznat dočasné pozastavení vylučovacího účinku, který má unijní právní pravidlo vůči vnitrostátnímu právu, které je v rozporu s tímto pravidlem. Takové omezení časové působnosti výkladu tohoto práva ze strany Soudního dvora lze připustit pouze v samotném rozsudku, kterým se rozhoduje o požadovaném výkladu [v tomto smyslu viz rozsudky ze dne 23. října 2012, Nelson a další, C-581/10 a C-629/10, EU:C:2012:657, body 89 a 91; ze dne 23. dubna 2020, Herst, C-401/18, EU:C:2020:295, body 56 a 57, a ze dne 25. června 2020, A a další (Větrné elektrárny v Aalter a v Nevele), C-24/19, EU:C:2020:503, bod 84 a citovaná judikatura].
- 217 Pokud by byly vnitrostátní soudy oprávněny přiznat vnitrostátním ustanovením přednost, byť dočasnou, před unijním právem, s nímž jsou v rozporu, byla by tím narušena přednost a jednotné používání unijního práva (v tomto smyslu viz rozsudek ze dne 29. července 2019, Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, bod 177 a citovaná judikatura).
- 218 Soudní dvůr nicméně ve věci, ve které se jednalo o legalitu opatření přijatých v rozporu s povinností – stanovenou unijním právem – provést předchozí posouzení vlivů záměru na životní prostředí a chráněnou lokalitu, rozhodl, že pokud to vnitrostátní právo umožňuje, může vnitrostátní soud výjimečně zachovat účinky takových opatření, pokud je toto zachování odůvodněno naléhavými důvody souvisejícími s nezbytností odvrátit skutečnou a vážnou hrozbu přerušení dodávek elektřiny dotyčného členského státu, již nelze čelit jinými prostředky a alternativními řešeními zejména v rámci vnitřního trhu, přičemž takové zachování se může vztahovat pouze na časový úsek, který je striktně nezbytný k nápravě protiprávnosti (v tomto smyslu viz rozsudek ze dne 29. července 2019, Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, body 175, 176, 179 a 181).

- 219 Na rozdíl od opomenutí takové procesní povinnosti, jako je předchozí posouzení vlivů záměru ve specifické oblasti ochrany životního prostředí, nemůže porušení čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny být předmětem nápravy postupem srovnatelným s postupem uvedeným v předchozím bodě. Zachování účinků takových vnitrostátních právních předpisů, jako jsou předpisy dotčené ve věci v původním řízení, by totiž znamenalo, že tyto právní předpisy nadále ukládají poskytovatelům služeb elektronických komunikací povinnosti, které jsou v rozporu s unijním právem a které znamenají závažné zásahy do základních práv osob, jejichž údaje byly uchovávány.
- 220 Předkládající soud tudíž nemůže uplatnit ustanovení svého vnitrostátního práva opravňující jej k tomu, aby časově omezil účinky prohlášení protiprávnosti, které mu přísluší podle tohoto práva, ve vztahu k vnitrostátním právním předpisům dotčeným ve věci v původním řízení.
- 221 VZ, WY a XX ovšem ve svých vyjádřeních předložených Soudnímu dvoru tvrdí, že třetí otázka se implicitně, avšak nutně zabývá tím, zda unijní právo brání tomu, aby byly v trestním řízení využity informace a důkazy získané prostřednictvím plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů neslučitelným s tímto právem.
- 222 V tomto ohledu a za účelem poskytnutí užitečné odpovědi předkládajícímu soudu je třeba připomenout, že za současného stavu unijního práva v zásadě přísluší pouze vnitrostátnímu právu, aby stanovilo pravidla přípustnosti a hodnocení – v rámci trestního řízení zahájeného proti osobám podezřelým ze závažné trestné činnosti – informací a důkazů získaných takovým uchováváním údajů, které je v rozporu s unijním právem.
- 223 Podle ustálené judikatury totiž platí, že při neexistenci unijní právní úpravy v dané oblasti je na vnitrostátním právním řádu každého členského státu, aby na základě zásady procesní autonomie upravil procesní podmínky soudních řízení určených k zajištění ochrany práv, která právním subjektům vyplývají z unijního práva, přičemž tyto podmínky nesmějí být méně příznivé než ty, které se týkají obdobných řízení na základě vnitrostátního práva (zásada rovnocennosti), ani upravené takovým způsobem, aby v praxi znemožňovaly nebo nadměrně ztěžovaly výkon práv přiznaných unijním právním řádem (zásada efektivity) (v tomto smyslu viz rozsudky ze dne 6. října 2015, Târșia, C-69/14, EU:C:2015:662, body 26 a 27; ze dne 24. října 2018, XC a další, C-234/17, EU:C:2018:853, body 21 a 22 a citovaná judikatura, a ze dne 19. prosince 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, bod 33).
- 224 Co se týče zásady rovnocennosti, je věcí vnitrostátního soudu, který rozhoduje v trestním řízení založeném na informacích či důkazech získaných v rozporu s požadavky vyplývajícími ze směrnice 2002/58, aby ověřil, zda vnitrostátní právo upravující toto řízení stanoví méně příznivá pravidla pro přípustnost a využití takových informací a důkazů, než jsou pravidla upravující informace a důkazy získané v rozporu s vnitrostátním právem.
- 225 Co se týče zásady efektivity, je třeba poukázat na to, že vnitrostátní pravidla týkající se přípustnosti a využití informací a důkazů mají na základě vnitrostátních právních mechanismů za cíl zabránit tomu, aby protiprávně získané informace a důkazy neprávem způsobily újmu osobě podezřelé ze spáchání trestných činů. Tohoto cíle přitom může být podle vnitrostátního práva dosaženo nejen zákazem využití takových informací a důkazů, ale rovněž vnitrostátními pravidly a zvyklostmi upravujícími hodnocení a vážení informací a důkazů, nebo také zohledněním jejich protiprávní povahy při stanovování trestu.
- 226 Z judikatury Soudního dvora však vyplývá, že nezbytnost vyloučit informace a důkazy získané v rozporu s požadavky unijního práva musí být posuzována zejména s ohledem na riziko, které přípustnost takových informací a důkazů představuje pro dodržení zásady kontradiktornosti, a tudíž práva na spravedlivý proces (v tomto smyslu viz rozsudek ze dne 10. dubna 2003, Steffensen, C-276/01, EU:C:2003:228, body 76 a 77). Soud, který má za to, že účastník řízení se nemůže účinně

vyjádřit k důkaznímu prostředku, který spadá do oblasti, jež se vymyká znalosti soudu, a který může rozhodujícím způsobem ovlivnit posouzení skutkového stavu, musí konstatovat porušení práva na spravedlivý proces a vyloučit tento důkazní prostředek, aby takovému porušení zabránil (v tomto smyslu viz rozsudek ze dne 10. dubna 2003, Steffensen, C-276/01, EU:C:2003:228, body 78 a 79).

227 Zásada efektivity tudíž ukládá vnitrostátnímu trestnímu soudu, aby v trestním řízení zahájeném proti osobám podezřelým ze spáchání trestných činů nepřihlížel k informacím a důkazům, které byly získány prostřednictvím plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů neslučitelného s unijním právem, pokud se tyto osoby nemohou účinně vyjádřit k těmto informacím a důkazům, které spadají do oblasti, jež se vymyká znalosti soudu, a mohou zásadním způsobem ovlivnit posouzení skutkového stavu.

228 S ohledem na všechny výše uvedené úvahy je třeba na třetí otázku ve věci C-520/18 odpovědět, že vnitrostátní soud nemůže uplatnit ustanovení svého vnitrostátního práva opravňující jej k tomu, aby časově omezil účinky prohlášení protiprávnosti, které mu přísluší podle tohoto práva, ve vztahu k vnitrostátním právním předpisům, jež poskytovatelům služeb elektronických komunikací ukládají, zejména za účelem zajištění národní bezpečnosti a boje proti trestné činnosti, povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů, která je neslučitelná s čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny. Článek 15 odst. 1 uvedené směrnice vykládaný ve světle zásady efektivity ukládá vnitrostátnímu trestnímu soudu, aby v trestním řízení zahájeném proti osobám podezřelým ze spáchání trestných činů nepřihlížel k informacím a důkazům, které byly získány prostřednictvím plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů neslučitelného s unijním právem, pokud se tyto osoby nemohou účinně vyjádřit k těmto informacím a důkazům, které spadají do oblasti, jež se vymyká znalosti soudu, a mohou zásadním způsobem ovlivnit posouzení skutkového stavu.

K nákladům řízení

229 Vzhledem k tomu, že řízení má, pokud jde o účastníky původních řízení, povahu incidenčního řízení ve vztahu ke sporům probíhajícím před předkládajícími soudy, jsou k rozhodnutí o nákladech řízení příslušné uvedené soudy. 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 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 články 7, 8 a 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie musí být vykládán v tom smyslu, že brání legislativním opatřením, která pro účely stanovené v čl. 15 odst. 1 preventivně stanoví plošné a nerozlišující uchovávání provozních a lokalizačních údajů. Naproti tomu čl. 15 odst. 1 směrnice 2002/58, ve znění směrnice 2009/136, ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny základních práv nebrání legislativním opatřením,

- která za účelem zajištění národní bezpečnosti stanoví možnost přikázat poskytovatelům služeb elektronických komunikací, aby prováděli plošné a nerozlišující uchovávání provozních a lokalizačních údajů v situacích, kdy dotýčný členský stát čelí závažnému ohrožení národní bezpečnosti, které se jeví jako skutečné a aktuální nebo předvídatelné, přičemž rozhodnutí o uložení tohoto příkazu může být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, a cílem tohoto

přezkumu bude ověřit, že nastala některá z těchto situací, jakož i dodržení podmínek a záruk, které musí být stanoveny, a tento příkaz však může být vydán pouze na dobu nezbytně nutnou, avšak s možností prodloužení, pokud ohrožení přetrvává;

- která za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti stanoví cílené uchovávání provozních a lokalizačních údajů, které je na základě objektivních a nediskriminačních kritérií vymezeno kategoriemi dotčených osob nebo prostřednictvím zeměpisného kritéria, na dobu nezbytně nutnou, avšak s možností prodloužení;
- která za účelem zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti stanoví plošné a nerozlišující uchovávání IP adres přidělených zdroji připojení, a to po nezbytně nutnou dobu;
- která za účelem zajištění národní bezpečnosti, boje proti trestné činnosti a veřejné bezpečnosti stanoví plošné a nerozlišující uchovávání údajů o totožnosti uživatelů prostředků elektronické komunikace a
- která za účelem boje proti závažné trestné činnosti a *a fortiori* zajištění národní bezpečnosti stanoví možnost přikázat rozhodnutím příslušného orgánu, které podléhá účinnému soudnímu přezkumu, poskytovatelům služeb elektronických komunikací, aby po určenou dobu prováděli urychlené uchování provozních a lokalizačních údajů, jimiž disponují,

pokud tato opatření pomocí jasných a přesných pravidel zajišťují při uchovávání dotčených údajů dodržení souvisejících hmotněprávních a procesních podmínek a pokud subjekty údajů mají k dispozici účinné záruky proti riziku zneužití.

2) Článek 15 odst. 1 směrnice 2002/58, ve znění směrnice 2009/136, nahlížený ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny základních práv, musí být vykládán v tom smyslu, že nebrání vnitrostátní právní úpravě, která ukládá poskytovatelům služeb elektronických komunikací, aby prováděli jednak automatizovanou analýzu a shromažďování zejména provozních a lokalizačních údajů v reálném čase a jednak shromažďování technických údajů o umístění používaných koncových zařízení v reálném čase, pokud

- je provádění automatizované analýzy omezeno na situace, kdy členský stát čelí závažné hrozbě pro národní bezpečnost, která se jeví jako skutečná a aktuální či předvídatelná, přičemž provádění této analýzy může být předmětem účinného přezkumu soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, a cílem takového přezkumu bude ověřit, že nastala situace, která uvedené opatření odůvodňuje, jakož i dodržení podmínek a záruk, které musí být stanoveny, a
- je provádění shromažďování provozních a lokalizačních údajů v reálném čase omezeno na subjekty, u nichž existuje pádný důvod se domnívat, že jsou určitým způsobem zapojeny do teroristických činností, a podléhá předchozímu přezkumu prováděnému soudem nebo nezávislým správním orgánem, jehož rozhodnutí je závazné, aby bylo zajištěno, že takové shromažďování v reálném čase bude povoleno pouze v mezích toho, co je nezbytně nutné. V řádně odůvodněných naléhavých případech musí být přezkum proveden v co nejkratší době.

3) Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) musí být vykládána v tom smyslu, že se nevztahuje na oblast ochrany důvěrnosti komunikace a fyzických osob v souvislosti se

zpracováním osobních údajů v rámci služeb informační společnosti, jelikož tato ochrana je upravena – podle okolností – směrnicí 2002/58, ve znění směrnice 2009/136, nebo 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. Článek 23 odst. 1 nařízení 2016/679 nahlížený ve světle článků 7, 8 a 11 a čl. 52 odst. 1 Listiny základních práv musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která poskytovatelům veřejných komunikačních služeb on-line a poskytovatelům hostingových služeb ukládá povinnost plošného a nerozlišujícího uchovávání údajů, zejména osobních údajů souvisejících s těmito službami.

- 4) Vnitrostátní soud nemůže uplatnit ustanovení svého vnitrostátního práva opravňující jej k tomu, aby časově omezil účinky prohlášení protiprávnosti, které mu přísluší podle tohoto práva, ve vztahu k vnitrostátním právním předpisům, jež poskytovatelům služeb elektronických komunikací ukládají, zejména za účelem zajištění národní bezpečnosti a boje proti trestné činnosti, povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů, která je neslučitelná s článkem 15 odst. 1 směrnice 2002/58, ve znění směrnice 2009/136, ve spojení s články 7, 8 a 11 a čl. 52 odst. 1 Listiny. Článek 15 odst. 1 uvedené směrnice vykládaný ve světle zásady efektivity ukládá vnitrostátními trestnímu soudu, aby v trestním řízení zahájeném proti osobám podezřelým ze spáchání trestných činů nepřihlížel k informacím a důkazům, které byly získány prostřednictvím plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů neslučitelného s unijním právem, pokud se tyto osoby nemohou účinně vyjádřit k těmto informacím a důkazům, které spadají do oblasti, jež se vymyká znalosti soudu, a mohou zásadním způsobem ovlivnit posouzení skutkového stavu.

Podpisy.