Sbírka soudních rozhodnutí

STANOVISKO GENERÁLNÍHO ADVOKÁTA
MANUELA CAMPOS SÁNCHEZ-BORDONY
přednesené dne 15. ledna 2020[1]

Spojené věci C-511/18 a C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
proti
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[žádost o rozhodnutí o předběžné otázce podaná Conseil d'État (Státní rada, jednající jako nejvyšší správní soud, Francie)]

„Řízení o předběžné otázce – Zpracovávání osobních údajů a ochrana soukromí v odvětví elektronických komunikací – Zachování národní bezpečnosti a boj proti terorismu – Směrnice 2002/58/ES – Oblast působnosti – Článek 1 odst. 3 – Článek 15 odst. 3 – Článek 4 odst. 2 SEU – Listina základních práv Evropské unie – Články 6, 7, 8, 11, 47 a čl. 52 odst. 1 – Plošné a nerozlišující uchovávání údajů o připojení a údajů umožňujících zjistit totožnost tvůrců obsahu – Sběr provozních a lokalizačních údajů – Přístup k údajům"

1. Soudní dvůr v posledních letech drží v oblasti uchovávání osobních údajů a přístupu k nim ustálenou judikaturu, v jejímž rámci zvláště vynikají:

– rozsudek ze dne 8. dubna 2014, Digital Rights Ireland a další[2], v němž konstatoval neplatnost směrnice 2006/24/ES[3] z důvodu, že umožňovala nepřiměřený zásah do práv zakotvených v článcích 7 a 8 Listiny základních práv Evropské unie (dále jen „Listina");

– rozsudek ze dne 21. prosince 2016, Tele2 Sverige a Watson a další[4], v němž vyložil čl. 15 odst. 1 směrnice 2002/58/ES[5];

1 – Původní jazyk: španělština.

2 – Věci C-293/12 a C-594/12, dále jen „rozsudek Digital Rights", EU:C:2014:238.

3 – Směrnice Evropského parlamentu a Rady 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).

4 – Věci C-203/15 a C-698/15, dále jen „rozsudek Tele2 Sverige a Watson", EU:C:2016:970.

5 – Směrnice Evropského parlamentu a Rady 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).

– rozsudek ze dne 2. října 2018, Ministerio Fiscal[6], v němž potvrdil výklad tohoto ustanovení směrnice 2002/58.

2. Tyto rozsudky (zejména druhý z uvedených) znepokojují orgány některých členských států, neboť podle jejich názoru byly v důsledku těchto rozsudků zbaveny nástroje, který považují za nezbytný pro zachování národní bezpečnosti a pro boj proti kriminalitě a terorismu. Některé z těchto států tak usilují o překonání či upřesnění této judikatury.

3. Soudy členských států vyjádřily uvedené znepokojení ve čtyřech žádostech o rozhodnutí o předběžné otázce[7], k nimž přednáším stanovisko týž den.

4. Ve všech čtyřech věcech vyvstává především otázka použitelnosti směrnice 2002/58 na činnosti týkající se národní bezpečnosti a boje proti terorismu. V případě, že by se za těchto okolností směrnice použila, mělo by být následně objasněno, do jaké míry mohou členské státy omezit právo na soukromí, jež daná směrnice chrání. A konečně bude nutné analyzovat, do jaké míry jsou vnitrostátní právní úpravy (britská[8], belgická[9] a francouzská[10]) v této oblasti v souladu s unijním právem, jak bylo vyloženo Soudním dvorem.

I. Právní rámec

A. Unijní právo

1. Směrnice 2002/58

5. Článek 1 („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 ve Společenství.

[…]

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

6. Článek 3 („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.“

6 – Věc C-207/16, dále jen „rozsudek Ministerio Fiscal“, EU:C:2018:788.

7 – Kromě projednávaných dvou (věci C-511/18 a C-512/18) se jedná o věci C-623/17, Privacy International, a C-520/18, Ordre des barreaux francophones et germanophone a další.

8 – Věc Privacy International, C-623/17.

9 – Věc Ordre des barreaux francophones et germanophone a další, C-520/18.

10 – Věci La Quadrature du Net a další, C-511/18 a C-512/18.

7. Článek 5 („Důvěrný charakter sdělení“) v odstavci 1 stanoví:

„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.“

8. Článek 6 („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.“

9. Článek 15 („Použití některých ustanovení směrnice 95/46/ES[[11]“) v odstavci 1 stanoví:

„Členské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/46/ES. 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 Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o Evropské unii.“

2. Směrnice 2000/31/ES [12]

10. Článek 14 stanoví:

„1. Členské státy zajistí, aby v případě služby informační společnosti spočívající v ukládání informací poskytovaných příjemcem služby nebyl poskytovatel služby odpovědný za informace ukládané na žádost příjemce, pokud:

[…]

3. Tímto článkem není dotčena možnost soudního nebo správního orgánu požadovat od poskytovatele služby v souladu s právním řádem členských států, aby ukončil protiprávní jednání nebo mu předešel, ani možnost členských států zavést postupy, které umožní odstranění nebo znemožní přístup k informaci.“

11 – Směrnice Evropského parlamentu a Rady 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).

12 – Směrnice Evropského parlamentu a Rady 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. 13/25, s. 399).

11. Článek 15 zní:

„1. Členské státy neukládají poskytovatelům služeb uvedených v článcích 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 služeb [příjemci jejich 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.“

3. Nařízení (EU) 2016/679[13]

12. Článek 2 („Věcná působnost“) 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;

c) fyzickou osobou v průběhu výlučně osobních či domácích činností;

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

[…]“

13. Článek 23 odst. 1 („Omezení“) stanoví:

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

a) národní bezpečnost;

b) obranu;

c) veřejnou bezpečnost;

13 – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. 2016, L 119, s. 1).

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

e) jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu, včetně peněžních, 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.“

14. Článek 95 („Vztah ke směrnici 2002/58/ES“) 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 týmž cílem stanovené ve směrnici 2002/58/ES.“

B. Vnitrostátní právo

1. Code de la sécurité intérieure (zákoník vnitřní bezpečnosti)

15. Článek L. 851-1 stanoví:

„Za podmínek stanovených v kapitole 1 hlavy II této části může být u provozovatelů elektronických komunikací a osob uvedených v článku L. 34-1 code des postes et des communications électroniques [(zákoník poštovních služeb a elektronických komunikací)], jakož i osob uvedených v odstavcích 1 a 2 bodu I článku 6 loi n.º 2004-575 […] pour la confiance dans l'économie numérique [(zákon č. 2004-575 […] o posílení důvěry v digitální ekonomiku)] povolen sběr 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, identifikace všech účastnických nebo připojovacích čísel určené osoby, umístění použitého koncového zařízení a komunikace účastníka v podobě seznamu volaných a volajících čísel, délky trvání a data komunikace. […]“

16. Články L. 851-2 a L. 851-4 upravují přístup správních orgánů v reálném čase k takto uchovaným údajům o připojení v závislosti na jednotlivých různých účelech a podmínkách.

17. Podle článku L. 851-2 je dovoleno sbírat od týchž osob informace nebo dokumenty zmíněné v článku L. 851-1 výhradně pro účely předcházení terorismu. Tento sběr, zaměřený na jednu či více osob předem identifikovaných jako osoby, jež mohou mít vazbu na hrozbu terorismu, probíhá v reálném čase. Stejně je tomu v případě článku L. 851-4, který umožňuje, aby provozovatelé

v reálném čase předávali pouze technické údaje o poloze koncových zařízení [14].

18. Článek L. 851-3 stanoví možnost uložit provozovatelům elektronických komunikací a poskytovatelům technických služeb 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“ [15].

19. V článku L. 851-5 se upřesňuje, že za určitých podmínek „lze povolit použití technického zařízení umožňujícího lokalizovat v reálném čase určitou osobu, určité vozidlo nebo určitý předmět“.

20. Podle čl. L. 851-6 odst. I lze za jistých podmínek „přímo, prostřednictvím přístroje nebo technického zařízení zmíněného v bodě 1 článku 226-3 code pénal [(trestní zákoník)], shromažďovat technické údaje o připojení umožňující identifikovat koncové zařízení nebo účastnické číslo jeho uživatele, jakož i údaje o umístění použitých koncových zařízení“.

2. Zákoník poštovních služeb a elektronických komunikací

21. Podle článku L. 34-1, ve znění účinném v době rozhodné z hlediska skutkového stavu, platilo:

„I. Tento článek se vztahuje na zpracovávání osobních údajů při poskytování služeb elektronických komunikací veřejnosti; zejména se vztahuje na sítě podporující zařízení pro shromažďování a identifikaci údajů.

II. Aniž jsou dotčena ustanovení odstavců III, IV, V a VI, provozovatelé elektronických komunikací, a zejména osoby, jejichž činnost spočívá v poskytování on-line přístupu veřejnosti ke komunikačním službám, 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 upravených v článcích 323-1 a 323-3-1 trestního zákoníku a stíhaných podle těchto článků a za jediným 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 Commission nationale de l'informatique et des libertés [(Národní komise pro informační technologie a svobody)] se v mezích stanovených v odstavci VI určí tyto kategorie údajů a doba, po kterou jsou uchovávány, v závislosti na činnosti provozovatelů a povahy sdělení, jakož i pravidla náhrady případných dodatečných identifikovatelných a specifických nákladů vzniklých provozovatelům v souvislosti se službami poskytnutými k tomuto účelu na žádost státu.

14 – Podle předkládajícího soudu neukládají tyto metody poskytovatelům služeb povinnost dalšího uchovávání vedle toho, které je nezbytné pro účtování jejich služeb, prodeje těchto služeb a poskytování služeb s přidanou hodnotou.

15 – Podle předkládajícího soudu slouží tato metoda, která neobnáší plošné a nerozlišující uchovávání, pouze k tomu, že během omezené doby jsou ze všech údajů o připojení zpracovávaných těmito osobami sbírány ty údaje, které by mohly mít souvislost se závažným trestným činem tohoto typu.

[…]

VI. Údaje uchovávané a zpracovávané 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, sdělení vyměňovaných nebo informací vyhledaných 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 využití těchto údajů k účelům jiným než stanoveným v tomto článku."

22. Podle čl. R. 10-13 odst. I jsou provozovatelé povinni uchovávat pro účely vyšetřování, odhalování a stíhání trestných činů následující údaje:

„a) informace umožňující zjistit totožnost uživatele;

b) údaje o použitých komunikačních koncových zařízeních;

c) technické charakteristiky, jakož i datum, čas a délku trvání každé komunikace;

d) údaje o vyžádaných nebo využívaných doplňkových službách a jejích poskytovatelích;

e) údaje umožňující zjistit totožnost adresáta nebo adresáty sdělení."

23. Podle odstavce II téhož článku musí provozovatel v případě poskytování telefonních služeb uchovávat dále také údaje umožňující identifikovat zdroj a lokalizaci komunikace.

24. Podle odstavce III téhož článku musí být uvedené údaje uchovávány po dobu jednoho roku ode dne, kdy byly zaznamenány.

3. Loi n.º 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)

25. První pododstavec bodu II článku 6 zákona č. 2004-575 stanoví, že osoby, jejichž činností je poskytování přístupu veřejnosti ke komunikačním službám on-line, a fyzické či právnické osoby, které i bezúplatně nabízejí veřejnosti služby veřejné komunikace on-line, ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb, „drží a uchovávají údaje, na jejichž základě lze zjistit totožnost kohokoli, kdo přispěl k vytváření obsahu nebo části obsahu poskytovaných služeb".

26. Podle třetího pododstavce bodu II může justiční orgán od těchto osob požadovat sdělení údajů podle prvního pododstavce.

27. Poslední pododstavec bodu II stanoví, že nařízením vlády přijatým na základě stanoviska Conseil d'État (Státní rada) „se určí údaje uvedené v prvním pododstavci a stanoví doba a podmínky jejich uchovávání“ [16].

II. Skutkové okolnosti původních řízení a předběžné otázky

A. Věc C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net a Fédération des fournisseurs d'accès à internet associatifs (dále jen „navrhovatelé“) podali ke Conseil d'État (Státní rada) návrh na zrušení několika nařízení vlády provádějících některá ustanovení zákoníku vnitřní bezpečnosti [17].

29. Navrhovatelé v podstatě tvrdili, že napadená nařízení vlády i uvedená ustanovení zákoníku vnitřní bezpečnosti jsou v rozporu s právem na respektování soukromého života zaručeným článkem 7 Listiny, právem na ochranu osobních údajů zaručeným článkem 8 Listiny a právem na účinný právní prostředek zaručeným článkem 47 Listiny.

30. Za těchto podmínek předkládá Conseil d'État (Státní rada) Soudnímu dvoru následující 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 trvajícího ohrožení národní bezpečnosti, a zejména rizika terorismu tak, že jde o zásah odůvodněný právem na bezpečnost, které je zaručeno článkem 6 Listiny základních práv Evropské unie, a požadavky národní bezpečnosti, za kterou podle článku 4 [SEU] 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 v reálném čase, která mají současně dopad na práva a povinnosti poskytovatelů služeb elektronických komunikací, ale neukládají jim zvláštní povinnost uchovávání údajů?

16 – Toto určení bylo provedeno v 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). V tomto nařízení vlády stojí za pozornost a) čl. 1 bod 1, podle něhož mají osoby, které poskytují přístup ke komunikačním službám on-line, povinnost uchovávat následující údaje: identifikátor připojení, identifikátor přidělený danému účastníkovi, identifikátor koncového zařízení použitého k připojení, datum a čas zahájení a ukončení připojení, charakteristiky účastnického vedení; b) čl. 1 bod 2, podle něhož mají osoby, které i bezúplatně nabízejí veřejnosti služby veřejné komunikace on-line, ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb, povinnost uchovávat u jednotlivých operací následující údaje: identifikátor připojení u zdroje komunikace, identifikátor přidělený obsahu, jenž je předmětem operace, typy protokolů použitých pro připojení ke službě a pro přenos obsahu, povahu operace, datum a čas operace, identifikátor použitý autorem operace; a konečně c) čl. 1 bod 3, jenž stanoví, že osoby uvedené v předchozích dvou bodech mají povinnost uchovávat následující informace poskytnuté uživatelem při uzavření smlouvy nebo vytvoření účtu: identifikátor připojení při vytváření účtu, jméno a příjmení nebo název, příslušné poštovní adresy, použité pseudonymy, příslušné adresy elektronické pošty nebo účtu, telefonní čísla, aktuální heslo a údaje umožňující jej ověřit nebo změnit.

17 – Návrh se týká těchto nařízení vlády: a) 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); b) décret n.° 2015-1211 du 1er 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 využití zpravodajských metod podléhajících povolení a evidencí týkajících se bezpečnosti státu); c) 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 libre 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), a d) 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).

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 dotčené osoby, 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?“

B. Věc C-512/18

31. Navrhovatelé ve sporu, v rámci kterého bylo zahájeno řízení ve věci C-511/18, s výjimkou sdružení Igwan.net, podali ke Conseil d'État (Státní rada) také návrh na zrušení rozhodnutí, jímž byl (implicitně) zamítnut jejich návrh na zrušení článku R. 10-13 zákoníku poštovních služeb a elektronických komunikací a nařízení vlády č. 2011-219 ze dne 25. února 2011.

32. Podle názoru těchto navrhovatelů ukládají napadené předpisy povinnost uchovávat provozní a lokalizační údaje, jakož i údaje o připojení, která s ohledem na svou obecnost představuje nepřiměřený zásah do práva na respektování soukromého života zaručeného článkem 7 Listiny, práva na ochranu osobních údajů zaručeného článkem 8 Listiny a práva na svobodu projevu zaručeného článkem 11 Listiny, a to v rozporu s čl. 15 odst. 1 směrnice 2002/58.

33. V tomto řízení pokládá Conseil d'État (Státní rada) 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 zejména s ohledem na záruky a kontroly, k nimž patří shromažďování a využívání údajů o připojení, tak, že jde o zásah odůvodněný právem na bezpečnost, které je zaručeno článkem 6 Listiny základních práv Evropské unie, a požadavky národní bezpečnosti, za které podle článku 4 [SEU] nesou odpovědnost výhradně členské státy?

2) Musí být ustanovení směrnice [2000/31] […] nahlížená ve světle článků 6, 7, 8 a 11, jakož i čl. 52 odst. 1 Listiny […] vykládána v tom smyslu, že umožňují členskému státu přijmout vnitrostátní právní úpravu ukládající osobám, jejichž činností je poskytování přístupu veřejnosti ke komunikačním službám on-line, a fyzickým či právnickým osobám, které i bezúplatně nabízejí veřejnosti služby veřejné komunikace 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?“

III. Řízení před Soudním dvorem a stanoviska účastníků řízení

34. Žádosti o rozhodnutí o předběžné otázce byly zapsány do rejstříku kanceláře Soudního dvora dne 3. srpna 2018.

35. Písemná vyjádření předložily La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs a French Data Network, dále belgická, česká, dánská, německá, estonská, irská, španělská, francouzská, kyperská, maďarská, polská a švédská vláda a vláda Spojeného království, jakož i Komise.

36. Dne 9. září 2019 se konalo jednání společné s jednáním ve věcech C-623/17, Privacy International, a C-520/18, Ordre des barreaux francophones et germanophone a další, jehož se zúčastnili účastníci všech čtyř řízení o předběžné otázce, výše uvedené vlády a vlády Nizozemska a Norska, jakož i Komise a Evropský inspektor ochrany údajů.

IV. Analýza

37. Otázky Conseil d'État (Státní rada) lze shrnout do tří:

– zaprvé zda je s unijním právem slučitelná taková vnitrostátní právní úprava, která poskytovatelům služeb elektronických komunikací ukládá povinnost plošně a nerozlišujícím způsobem uchovávat údaje o připojení (první otázka ve věci C-511/18 a ve věci C-512/18), a zejména údaje umožňující zjistit totožnost tvůrců obsahu nabízeného uvedenými poskytovateli (druhá otázka ve věci C-512/18);

– zadruhé zda legalita postupů sběru údajů o připojení závisí v každém případě na povinnosti vyrozumět dotčené osoby, jakmile již není ohroženo vyšetřování (třetí otázka ve věci C-511/18), a

– zatřetí zda sběr provozních a lokalizačních údajů v reálném čase bez povinnosti je uchovávat je, a za jakých podmínek, slučitelný se směrnicí 2002/58 (druhá otázka ve věci C-511/18).

38. V konečném důsledku je třeba určit, zda je v souladu s unijním právem taková vnitrostátní právní úprava, která poskytovatelům služeb elektronických komunikací ukládá dva druhy povinností, a sice jednak a) *sběr* určitých údajů, avšak nikoli jejich uchovávání, a jednak b) *uchovávání* údajů o připojení a údajů umožňujících zjistit totožnost tvůrců obsahu služeb poskytovaných takovými poskytovateli.

39. Předně bude třeba rozhodnout, zda právě s ohledem na kontext [18], ve kterém byla vnitrostátní právní úprava přijata (tzn. za okolností možného ohrožení národní bezpečnosti), je směrnice 2002/58 vůbec použitelná.

A. K použitelnosti směrnice 2002/58

40. Předkládající soud nepochybuje o tom, že sporná právní úprava spadá do oblasti působnosti směrnice 2002/58. Plyne to podle jeho názoru z judikatury zavedené rozsudkem Tele2 Sverige a Watson a potvrzené v rozsudku Ministerio Fiscal.

41. Některé vlády, které se zúčastnily tohoto řízení, mají naopak za to, že sporná právní úprava do oblasti působnosti této směrnice nespadá. Svůj názor opírají mimo jiné o rozsudek ze dne 30. května 2006, Parlament v. Rada a Komise [19].

42. S Conseil d'État (Státní rada) se ztotožňuji v tom, že v rozsudku Tele2 Sverige a Watson byla tato část debaty vyřešena s tím, že směrnice 2002/58 se v zásadě použije tehdy, když jsou poskytovatelé elektronických služeb podle zákona povinni uchovávat údaje svých účastníků a umožnit orgánům veřejné moci přístup k nim. Skutečnost, že povinnosti jsou poskytovatelům uloženy z důvodu národní bezpečnosti, na tomto závěru nic nemění.

43. Je přitom třeba předeslat, že kdyby se rozsudek Tele2 Sverige a Watson rozcházel se staršími rozsudky, přednost by coby pozdější musel dostat rozsudek Tele2 Sverige a Watson, jenž byl potvrzen rozsudkem Ministerio Fiscal. Mám nicméně za to, že rozsudky se nerozcházejí, a tento svůj názor se nyní pokusím vysvětlit.

18 – „[K]ontextu kontextu vážného a trvajícího ohrožení národní bezpečnosti, a zejména rizika terorismu“, jak je upřesněno v první otázce ve věci C-511/18.

19 – Věci C-317/04 a C-318/04, dále jen „rozsudek Parlament v. Rada a Komise“, EU:C:2006:346.

1. Rozsudek Parlament v. Rada a Komise

44. Věci, ve kterých bylo rozhodnuto rozsudkem Parlament v. Rada a Komise, se týkaly:

– dohody mezi Evropským společenstvím a Spojenými státy americkými o zpracování a předávání údajů jmenné evidence cestujících [Passenger Name Records (PNR)] leteckými dopravci americkým orgánům [20] a

– odpovídající úrovně ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají uvedeným orgánům [21].

45. Soudní dvůr dospěl k závěru, že předávání těchto údajů představuje zpracovávání, jehož účelem je veřejná bezpečnost a činnosti státu v oblasti trestního práva. V souladu s čl. 3 odst. 2 první odrážkou směrnice 95/46 byla obě sporná rozhodnutí vyloučena z oblasti působnosti směrnice 95/46.

46. Údaje byly leteckými dopravci původně sesbírány v rámci činnosti, která spadá do oblasti působnosti unijního práva, a sice v rámci prodeje letenek. Nicméně jejich zpracovávání, kterého se týkalo sporné rozhodnutí, není „nezbytné[…] k poskytování služeb, ale k zachování veřejné bezpečnosti a trestním účelům“ [22].

47. Soudní dvůr se tak přidržel teleologického přístupu zohledňujícího účel sledovaný zpracováním údajů s tím, že vzhledem k tomu, že sledovaným účelem je ochrana veřejné bezpečnosti, musí být považováno za vyloučené z oblasti působnosti směrnice 95/46. Tento účel ovšem nebyl jediným určujícím kritériem [23], neboť v rozsudku je zdůrazněno, že je „začleněn[…] do rámce zavedeného orgány veřejné moci týkajícího se veřejné bezpečnosti“ [24].

48. Na základě rozsudku Parlament v. Rada a Komise lze tedy zkoumat rozdíl mezi ustanovením směrnice 95/46 o výluce a ustanoveními téže směrnice o omezeních (která jsou obdobná ustanovením směrnice 2002/58). Je nicméně pravda, že se tato ustanovení obou směrnic zaměřují na podobné cíle obecného zájmu, což přispívá k jistému zmatení co do jejich působnosti, jak poznamenal již generální advokát Y. Bot [25].

20 – Rozhodnutí Rady 2004/496/ES ze dne 17. května 2004 o uzavření dohody mezi Evropským společenstvím a Spojenými státy americkými o zpracování a předávání údajů jmenné evidence cestujících (PNR) Úřadu pro cla a ochranu hranic ministerstva vnitřní bezpečnosti Spojených států (Úř. věst. 2004, L 183, s. 83) (věc C-317/04).

21 – Rozhodnutí Komise 2004/535/ES ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cla a ochranu hranic (Úř. věst. 2004, L 235, s. 11) (věc C-318/04).

22 – Rozsudek Parlament v. Rada a Komise, bod 57. V bodě 58 je kladen důraz na to, že ze „skutečnosti, že údaje […] byly shromážděny soukromými subjekty k obchodním účelům a že jsou to tyto soukromé subjekty, kdo organizuje jejich předávání třetím státům“, neplyne, že by dotčené předávání nebylo jednou z hypotéz vylučujících použití směrnice 95/46 uvedených v jejím čl. 3 odst. 2 první odrážce, neboť „[t]oto předávání je […] začleněno do rámce zavedeného orgány veřejné moci týkajícího se veřejné bezpečnosti“.

23 – Na to později poukázal, žel již zesnulý, generální advokát Y. Bot ve svém stanovisku ve věci Irsko v. Parlament a Rada (C-301/06, EU:C:2008:558). V něm uvedl, že rozsudek Parlament v. Rada a Komise „neznamená, že pouze zkoumání cíle sledovaného zpracováním osobních údajů je relevantní pro účel vyloučení nebo zahrnutí takového zpracování do působnosti systému ochrany osobních údajů zavedeného směrnicí 95/46. Je rovněž nezbytné určit, v průběhu jaké činnosti je zpracování údajů prováděno. Pouze tehdy, pokud se toto zpracování uskutečňuje v průběhu činností, které jsou vlastní státu nebo státním orgánům a nesouvisí s činností jednotlivců, je vyloučeno ze systému ochrany osobních údajů Společenství založeného na směrnici 95/46, a to na základě jejího čl. 3 odst. 2 první odrážky“ (bod 122).

24 – Rozsudek Parlament v. Rada a Komise, bod 58. Hlavním předmětem dohody bylo uložit leteckým dopravcům přepravujícím cestující mezi Unií a Spojenými státy, aby poskytli orgánům Spojených států elektronický přístup k údajům jmenné evidence cestujících obsaženým v jejich počítačových rezervačních a odbavovacích systémech. Zaváděla tedy jistou formu mezinárodní spolupráce mezi Unií a Spojenými státy za účelem boje proti terorismu a další závažné trestné činnosti úsilím o uvedení tohoto cíle do souladu s cílem ochrany osobních údajů cestujících. V tomto ohledu se povinnost uložená dopravcům příliš nelišila od přímé výměny údajů mezi orgány veřejné moci.

25 – Stanovisko generálního advokáta Y. Bota ve věci Irsko v. Parlament a Rada (C-301/06, EU:C:2008:558, bod 127).

49. Je pravděpodobné, že z tohoto zmatení vychází názor, který zastávají členské státy hájící nepoužitelnost směrnice 2002/58 na tento kontext. Podle jejich názoru lze zájem národní bezpečnosti zachovat jen prostřednictvím výluky stanovené v čl. 1 odst. 3 směrnice 2002/58. Témuž zájmu ovšem nepochybně slouží i omezení dovolená článkem 15 odst. 1 této směrnice, mezi něž patří omezení týkající se národní bezpečnosti. Posledně uvedené ustanovení by bylo zbytečné, kdyby použitelnost směrnice 2002/58 musela být vyloučena, kdykoli se poukáže na národní bezpečnost.

2. Rozsudek Tele2 Sverige a Watson

50. V rozsudku Tele2 Sverige a Watson byla projednávána otázka, zda jsou s unijním právem v souladu některé vnitrostátní režimy ukládající poskytovatelům veřejně dostupných služeb elektronických komunikací plošnou povinnost uchovávat údaje o těchto komunikacích. Skutkové okolnosti byly tedy v zásadě stejné jako v nyní projednávaných žádostech o rozhodnutí o předběžné otázce.

51. Soudní dvůr ke znovu nastolené otázce použitelnosti unijního práva – nyní již reprezentovaného směrnicí 2002/58 – předně uvedl, že „rozsah oblasti působnosti směrnice 2002/58 musí být posouzen zejména s ohledem na obecnou systematiku uvedené směrnice“ [26].

52. V tomto ohledu poukázal Soudní dvůr na to, že „[j]e jistě pravda, že se legislativní opatření uvedená v čl. 15 odst. 1 směrnice 2002/58 týkají činností, jež jsou vlastní státům nebo státním orgánům a nesouvisí s oblastmi činností jednotlivců […] Kromě toho se účely, které taková opatření musí na základě tohoto ustanovení naplňovat, jimiž je v projednávaných věcech zajištění národní bezpečnosti […], v podstatě kryjí s účely sledovanými činnostmi, na které se vztahuje čl. 1 odst. 3 této směrnice“ [27].

53. Účel opatření, která v souladu s čl. 15 odst. 1 směrnice 2002/58 mohou přijmout členské státy k omezení práva na soukromí, se tudíž (v tomto ohledu) kryje s účelem, který odůvodňuje vynětí některých činností státu z režimu směrnice na základě jejího čl. 1 odst. 3.

54. Soudní dvůr dospěl ovšem k názoru, že „s ohledem na celkovou systematiku směrnice 2002/58“ nelze na základě uvedené okolnosti „dospět k závěru, že oblast působnosti směrnice 2002/58 se nevztahuje na legislativní opatření uvedená v jejím čl. 15 odst. 1, nemá-li být toto ustanovení zcela zbaveno užitečného účinku. Uvedené ustanovení totiž nutně předpokládá, že vnitrostátní opatření, která jsou v něm uvedena, […] spadají do oblasti působnosti téže směrnice, neboť posledně uvedená směrnice výslovně opravňuje členské státy k jejich přijetí pouze tehdy, jsou-li dodrženy podmínky, které tato směrnice stanoví“ [28].

55. K tomu se připojuje skutečnost, že omezeními dovolenými článkem 15 odst. 1 směrnice 2002/58 „se pro účely, jež jsou uvedeny v tomto ustanovení, řídí činnost poskytovatelů služeb elektronických komunikací“. Proto musí být toto ustanovení ve spojení s článkem 3 uvedené směrnice „vykládán[o] v tom smyslu, že taková legislativní opatření spadají do oblasti působnosti této směrnice“ [29].

56. V důsledku toho dospěl Soudní dvůr k závěru, že do oblasti působnosti směrnice 2002/58 spadají jak legislativní opatření ukládající poskytovatelům „povinnost uchovávat provozní a lokalizační údaje, neboť tato činnost nutně zahrnuje zpracování osobních údajů ze strany těchto poskytovatelů“ [30], tak i legislativní opatření upravující přístup orgánů k údajům uchovávaným těmito poskytovateli [31].

26 – Rozsudek Tele2 Sverige a Watson, bod 67.

27 – Tamtéž, bod 72.

28 – Tamtéž, bod 73.

29 – Tamtéž, bod 74.

30 – Tamtéž, bod 75.

31 – Tamtéž, bod 76.

57. Způsob, jakým směrnici 2002/58 vyložil Soudní dvůr v rozsudku Tele2 Sverige a Watson, byl zopakován v rozsudku Ministerio Fiscal.

58. Lze s úspěchem tvrdit, že rozsudek Tele2 Sverige a Watson je – více či méně implicitním – odklonem od judikatury zavedené v rozsudku Parlament v. Rada a Komise? Tento argument hájí například vláda Irska, podle které je s právním základem směrnice 2002/58 a s čl. 4 odst. 2 SEU v souladu jen posledně zmíněný rozsudek [32].

59. Francouzská vláda se domnívá, že rozpor by bylo možné zhojit uvědoměním si skutečnosti, že judikatura vycházející z rozsudku Tele2 Sverige a Watson se týká činností členských států v oblasti trestního práva, zatímco judikatura vycházející z rozsudku Parlament v. Rada a Komise souvisí s bezpečností státu a obranou. Judikatura vycházející z rozsudku Tele2 Sverige a Watson se proto podle ní neuplatní na skutkové okolnosti projednávaných věcí, za kterých je třeba uplatnit řešení přijaté v rozsudku Parlament v. Rada a Komise [33].

60. Jak jsem již předeslal, podle mého názoru lze uvést oba rozsudky do souladu, avšak jinak, než jak navrhuje francouzská vláda. S jejími argumenty se neztotožňuji, protože podle mě se závěry z rozsudku Tele2 Sverige a Watson týkající se výslovně boje proti terorismu [34] dají vztáhnout na jakoukoli jinou hrozbu pro národní bezpečnost (přičemž terorismus je jen jednou z nich).

3. Možnost souladného výkladu rozsudku Parlament v. Rada a Komise a rozsudku Tele2 Sverige a Watson

61. V rozsudku Tele2 Sverige a Watson i v rozsudku Ministerio Fiscal Soudní dvůr podle mého názoru zohlednil smysl ustanovení o výluce a o omezení, jakož i systematický vztah mezi těmito dvěma typy ustanovení.

62. Jestliže Soudní dvůr ve věci Parlament v. Rada a Komise uvedl, že zpracovávání údajů nespadá do působnosti směrnice 95/46, bylo tomu tak proto, jak jsem již připomněl, že v kontextu spolupráce mezi Evropskou unií a Spojenými státy v typicky mezinárodním rámci musel být státní rozměr činnosti upřednostněn před skutečností, že uvedené zpracovávání mělo i soukromý, resp. obchodní rozměr. Jednou z tehdy projednávaných otázek byl právě náležitý právní základ sporného rozhodnutí.

63. Naproti tomu u vnitrostátních opatření posuzovaných v rozsudku Tele2 Sverige a Watson a v rozsudku Ministerio Fiscal se Soudní dvůr zaměřil primárně na interní dosah zpracovávání údajů, neboť vzhledem k tomu, že právní rámec, ve kterém k němu docházelo, byl čistě vnitrostátní, chyběl externí rozměr, kterým se vyznačoval předmět rozsudku Parlament v. Rada a Komise.

64. Rozdílný význam mezinárodního a vnitrostátního (obchodního a soukromého) rozměru zpracovávání údajů se v prvním případě projevil tím, že se ustanovení unijního práva o výluce prosadilo jako nejvhodnější k ochraně obecného zájmu národní bezpečnosti. Ve druhém případě bylo naopak možné tohoto cíle účinně dosáhnout prostřednictvím ustanovení o omezení podle čl. 15 odst. 1 směrnice 2002/58.

65. Počítat je ještě třeba i s dalším rozdílem, souvisejícím s odlišným normativním rámcem, a sice že tyto jednotlivé rozsudky byly zaměřeny na výklad dvou ustanovení, která – i když to tak na první pohled nemusí vypadat – nejsou stejná.

32 – Body 15 a 16 písemného vyjádření irské vlády.

33 – Body 34 až 50 písemného vyjádření francouzské vlády.

34 – Rozsudek Tele2 Sverige a Watson, body 103 a 119.

66. Rozsudek Parlament v. Rada a Komise se totiž týkal výkladu čl. 3 odst. 2 směrnice 95/46, zatímco rozsudek Tele2 Sverige a Watson výkladu čl. 1 odst. 3 směrnice 2002/58. Z pozorné četby těchto článků vyplývá odlišnost, která je dostatečnou oporou pro smysl rozhodnutí Soudního dvora v obou uvedených případech.

67. Článek 3 odst. 2 směrnice 95/46 stanoví, že „[t]ato směrnice *se nevztahuje na zpracování osobních údajů* […] prová[d]ěné pro výkon činností, které nespadají do oblasti působnosti práva Společenství […], 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“ [35].

68. Podle čl. 1 odst. 3 směrnice 2002/58 se tato směrnice „*nevztahuje na činnosti*, které nespadají do oblasti působnosti Smlouvy o založení Evropského společenství […], 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“ [36].

69. Zatímco čl. 3 odst. 2 směrnice 95/46 vylučuje *zpracování údajů*, jehož předmětem je – v souvislosti s projednávanými věcmi – bezpečnost státu, čl. 1 odst. 3 směrnice 2002/58 vylučuje *činnosti* zaměřené na – rovněž v souvislosti s projednávanými věcmi – bezpečnost státu.

70. Tato odlišnost není bezvýznamná. Směrnice 95/46 vylučovala z oblasti své působnosti činnost („zpracovávání osobních údajů“), kterou mohl provádět každý. Z této činnosti byla konkrétně vyňata zpracování, která se týkají mimo jiné bezpečnosti státu. Naproti tomu bylo irelevantní, jakou povahu měl *subjekt* zpracovávající údaje. K vymezení vyloučených činností se tedy přistupovalo teleologicky, resp. účelově, a bez rozlišování osob, které je provádějí.

71. Z uvedeného vyplývá, že ve věci Parlament v. Rada a Komise přihlížel Soudní dvůr primárně k účelu sledovanému zpracováním údajů. Nebyla podstatná „skutečnost[…], že údaje […] byly shromážděny soukromými subjekty k obchodním účelům a že jsou to tyto soukromé subjekty, kdo organizuje jejich předávání třetím státům“, protože klíčové bylo to, že „[t]oto předávání je […] začleněno do rámce zavedeného orgány veřejné moci týkajícího se veřejné bezpečnosti“ [37].

72. Naproti tomu „činnosti týkající se bezpečnosti státu“, jež stojí mimo oblast působnosti směrnice 2002/58 posuzovanou ve věci Tele2 Sverige a Watson, nemůže vykonávat jakýkoli subjekt, ale jen samotný stát. Navíc do nich nepatří normativní či regulační funkce státu, nýbrž výhradně jen konkrétní úkony orgánů veřejné moci.

73. Tyto *činnosti* uvedené v čl. 1 odst. 3 směrnice 2002/58 jsou totiž „v každém případě příkladem činností státu či státních orgánů, které se liší od činnosti jednotlivců“ [38]. Tyto „činnosti“ přitom nemohou mít normativní povahu. Kdyby tomu tak bylo, zůstaly by všechny předpisy přijaté členskými státy v souvislosti se zpracováním osobních údajů mimo oblast působnosti směrnice 2002/58, přinejmenším kdyby měly být odůvodněny svou nezbytností k zajištění bezpečnosti státu.

74. To by na jednu stranu vedlo k významné ztrátě efektivity uvedené směrnice, protože k vyloučení použitelnosti záruk, které unijní normotvůrce koncipoval k ochraně osobních údajů občanů, vůči členským státům by postačilo jednoduše odkázat na právní institut natolik neurčitý, jako je národní bezpečnost. Taková ochrana je neproveditelná bez přispění členských států a její zaručení je z pohledu občana zajišťováno i vůči vnitrostátním orgánům veřejné moci.

35 – Kurzivou zvýraznil autor stanoviska.

36 – Kurzivou zvýraznil autor stanoviska.

37 – Parlament v. Rada a Komise, bod 58.

38 – Rozsudek Ministerio Fiscal, bod 32. V tomtéž smyslu rozsudek Tele2 Sverige a Watson, bod 72.

75. Na druhou stranu by takový výklad pojmu „činnosti státu“, který by zahrnoval i činnosti projevující se ve vydávání norem a právních předpisů, zbavil smyslu článek 15 směrnice 2002/58, který právě zmocňuje členské státy k tomu, aby – mimo jiné z důvodů ochrany národní bezpečnosti – přijímaly „legislativní opatření“ s cílem omezit dosah některých práv a povinností upravených v téže směrnici [39].

76. Jak zdůraznil Soudní dvůr v rozsudku Tele2 Sverige a Watson, „rozsah oblasti působnosti směrnice 2002/58 musí být posouzen zejména s ohledem na obecnou systematiku uvedené směrnice“ [40]. V tomto ohledu je smysluplným a efektivitu zajišťujícím výkladem čl. 1 odst. 3 a čl. 15 odst. 1 směrnice 2002/58 takový výklad, podle kterého první z uvedených ustanovení představuje hmotněprávní výluku týkající se *činností* vykonávaných členskými státy v oblasti národní bezpečnosti (a rovnocenných oblastech) a druhé zmocnění k přijetí *legislativních opatření* (tedy obecně závazných předpisů), která v zájmu národní bezpečnosti dopadají na činnosti jednotlivců podléhající výkonu státní moci členských států a omezují práva zaručená směrnicí 2002/58.

4. Vyloučení národní bezpečnosti podle směrnice 2002/58

77. Národní bezpečnost (či její ekvivalent „bezpečnost státu“, jak je zdůrazněno v jejím čl. 15 odst. 1) zohledňuje směrnice 2002/58 ze dvou úhlů. Zaprvé představuje důvod pro *vyloučení* (z působnosti této směrnice) všech činností členských států „týkající[ch] se“ této bezpečnosti. Zadruhé odůvodňuje *omezení* práv a povinností uvedených ve směrnici 2002/58 – tj. ve vztahu k činnostem soukromé či obchodní povahy a nespadajícím do výsadních pravomocí státu – které musí být provedeno zákonem [41].

78. Na jaké činnosti se vztahuje čl. 1 odst. 3 směrnice 2002/58? Dle mého názoru nabízí Conseil d'État (Státní rada) dobrý příklad, když zmiňuje články L. 851-5 a L. 851-6 zákoníku vnitřní bezpečnosti a poukazuje na „metody sběru informací, které přímo používá stát, ale neupravují činnosti poskytovatelů služeb elektronických komunikací tak, že by jim ukládaly zvláštní povinnosti“ [42].

79. Domnívám se, že toto je klíčem k vymezení oblasti výluky podle čl. 1 odst. 3 směrnice 2002/58. Do její působnosti nebudou spadat *činnosti* směřující k zajištění národní bezpečnosti a prováděné přímo orgány veřejné moci bez vyžadování spolupráce jednotlivců, potažmo bez uložení jim povinností v rámci jejich podnikatelské činnosti.

80. Škála činností orgánů veřejné moci vyloučených z obecné úpravy zpracování osobních údajů musí být nicméně vykládána restriktivně. Konkrétně nelze pojem *„národní bezpečnost“*, za kterou je podle čl. 4 odst. 2 SEU odpovědný výhradně každý členský stát, vztahovat i na další více či méně příbuzné oblasti veřejného života.

81. Vzhledem k tomu, že v projednávaných žádostech o rozhodnutí o předběžné otázce jde o zapojení jednotlivců (tedy osob poskytujících uživatelům služby elektronických komunikací), nikoli o pouhý zásah ze strany státních orgánů, nebude nutné se zabývat vymezením rozsahu národní bezpečnosti v úzkém slova smyslu.

39 – Jen stěží by totiž bylo možno tvrdit, že na základě čl. 15 odst. 1 směrnice 2002/58 lze omezit stanovená práva a povinnosti, jež podle něj spadají do oblasti, která se na základě čl. 1 odst. 3 samotné směrnice v zásadě nachází – stejně jako oblast národní bezpečnosti – mimo oblast její působnosti. Jak uvedl Soudní dvůr v bodě 73 rozsudku Tele2 Sverige a Watson, čl. 15 odst. 1 směrnice 2002/58 „nutně předpokládá, že vnitrostátní opatření, která jsou v něm uvedena, […] spadají do oblasti působnosti téže směrnice, neboť posledně uvedená směrnice výslovně opravňuje členské státy k jejich přijetí pouze tehdy, jsou-li dodrženy podmínky, které tato směrnice stanoví“.

40 – Rozsudek Tele2 Sverige a Watson, bod 67.

41 – Jak mimochodem uvedl generální advokát H. Saugmandsgaard Øe ve svém stanovisku ve věci Ministerio Fiscal (C-207/16, EU:C:2018:300), bod 47, „je třeba nezaměňovat osobní údaje zpracovávané *přímo* v rámci činností spadajících do výsadních pravomocí státu v oblasti trestního práva a údaje zpracovávané v rámci obchodní činnosti poskytovatelem služeb elektronických komunikací, které *poté* využijí příslušné státní orgány“.

42 – Body 18 a 21 předkládacího usnesení ve věci C-511/18.

82. Domnívám se nicméně, že jako vodítko může sloužit kritérium rámcového rozhodnutí 2006/960/SVV [43], jehož čl. 2 písm. a) rozlišuje donucovací orgány v širším smyslu – mezi které patří „vnitrostátní policejní, celní nebo jiný orgán, který je podle vnitrostátního práva oprávněn odhalovat trestné činy nebo trestnou činnost, předcházet jim a vyšetřovat je a v souvislosti s tím vykonávat pravomoci a přijímat donucovací opatření“ – na jedné straně a „agentury nebo jednotky zabývající se zejména otázkami bezpečnosti státu“ na straně druhé [44].

83. V bodě 11 odůvodnění směrnice 2002/58 se uvádí, že „tato směrnice, obdobně jako směrnice 95/46[…], se netýká ochrany základních práv a svobod ve vztahu k činnostem, které se neřídí právem [Unie]“. Proto směrnice 2002/58 „nemění stávající rovnováhu mezi právem jednotlivce na soukromí a možností, aby členské státy přijaly opatření uvedená v čl. 15 odst. 1 této směrnice, která jsou nezbytná pro ochranu […] bezpečnosti státu […]“.

84. Směrnice 2002/58 totiž v souvislosti s pravomocemi členských států v oblasti národní bezpečnosti navazuje na směrnici 95/46. Předmětem ani jedné z nich není ochrana základních práv v této konkrétní oblasti, v níž se činnosti členských států „neřídí právem [Unie]“.

85. „Rovnováha“, o které se hovoří v uvedeném bodě odůvodnění, vychází z nutnosti respektovat pravomoci členských států v oblasti národní bezpečnosti tehdy, když je vykonávají *přímo a vlastními prostředky*. Naproti tomu v případě, kdy se – a to i z týchž důvodů národní bezpečnosti – vyžaduje spolupráce jednotlivců, kterým jsou uloženy určité povinnosti, vede tato okolnost k aktivaci působnosti jedné z oblastí (ochrana soukromí, kterou lze od těchto soukromých subjektů požadovat) upravené unijním právem.

86. Směrnice 95/46 i směrnice 2002/58 usilují o dosažení této rovnováhy tak, že dovolují možnost omezit práva jednotlivců prostřednictvím normativních opatření přijatých státy podle čl. 13 odst. 1 směrnice 95/46 a čl. 15 odst. 1 směrnice 2002/58. V tomto ohledu není mezi oběma směrnicemi žádný rozdíl.

87. Co se týče nařízení 2016/679, které upravuje (nový) obecný rámec ochrany osobních údajů, to se podle jeho čl. 2 odst. 2 nevztahuje na „zpracování osobních údajů“ prováděné členskými státy „při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU“.

88. Jestliže v této souvislosti bylo zpracování osobních údajů vymezeno ve směrnici 95/46 jen s ohledem na jeho účel, tedy bez ohledu na subjekt, který jej prováděl, nařízení 2016/679 vymezuje vyloučené zpracování jak s ohledem na jeho účel, tak s ohledem na subjekty jej provádějící, přičemž vyloučeno je zpracování prováděné členskými státy při výkonu *činností*, které nespadají do oblasti působnosti unijního práva [čl. 2 odst. 2 písm. a) a b)], a činnosti prováděné orgány *za účelem boje proti trestné činnosti a ochrany* před hrozbami pro veřejnou bezpečnost [45].

89. Určení těchto činností orgánů veřejné moci musí nutně být restriktivní, neboť jinak by unijní právní úprava v oblasti ochrany soukromí byla zbavena efektivity. Nařízení 2016/679 upravuje v článku 23 – v návaznosti na čl. 15 odst. 1 směrnice 2002/58 – možnost omezit *prostřednictvím legislativních opatření* práva a povinnosti v něm uvedené, jestliže je takové omezení nezbytné s cílem

43 – Rámcové rozhodnutí Rady ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie (Úř. věst. 2006, L 386, s. 89).

44 – V tomtéž smyslu rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech (Úř. věst. 2008, L 350, s. 60) v čl. 1 odst. 4 stanovilo, že tímto rámcovým rozhodnutím „nejsou dotčeny podstatné zájmy národní bezpečnosti nebo zvláštní zpravodajské činnosti v oblasti národní bezpečnosti“.

45 – Nařízení č. 2016/679 vylučuje totiž zpracování údajů prováděné členskými státy při výkonu *činnosti*, která nespadá do oblasti působnosti unijního práva, a činnosti prováděné orgány *za účelem ochrany* veřejné bezpečnosti.

zajistit, mimo jiné, národní bezpečnost, obranu či veřejnou bezpečnost. Znovu, kdyby ochrana těchto cílů stačila k vyloučení z působnosti nařízení 2016/679, bylo by nadbytečné uvádět bezpečnost státu jakožto jeden z důvodů, ze kterých lze prostřednictvím legislativního opatření omezit práva zaručená tímto nařízením.

90. Stejně jako v případě směrnice 2002/58 by nebylo logické, aby legislativní opatření upravená v článku 23 nařízení 2016/679 (které, opakuji, dovoluje státům omezit práva občanů na soukromí z důvodu bezpečnosti státu) spadala do oblasti jeho působnosti a zároveň aby oblast bezpečnosti státu vylučovala bez dalšího použitelnost samotného nařízení, což by znamenalo neuznat žádné subjektivní právo.

B. Potvrzení a možnosti rozvinutí judikatury Tele2 Sverige a Watson

91. Ve svém stanovisku ve věci C-520/18 provádím podrobnou analýzu [46] judikatury Soudního dvora v této oblasti a na základě této analýzy navrhuji, aby byla tato judikatura potvrzena, přičemž nabízím výklad k dotvoření jejího obsahu.

92. Z důvodu hospodárnosti nepovažuji za nezbytné reprodukovat zde tuto analýzu, a tak na ni jen odkazuji. Níže rozvedené úvahy k předběžným otázkám vzneseným Conseil d'Etat (Státní rada) je proto třeba vykládat s ohledem na východiska uvedená v příslušných částech stanoviska ve věci C-520/18.

C. Odpověď na předběžné otázky

1. K povinnosti uchovávat údaje (první předběžná otázka ve věcech C-511/18 a C-512/18 a druhá předběžná otázka ve věci C-512/18)

93. V souvislosti s povinností uchovávat údaje uloženou poskytovatelům služeb elektronických komunikací se předkládající soud konkrétně táže, zda

– tato povinnost, kterou lze uložit na základě čl. 15 odst. 1 směrnice 2002/58, představuje zásah odůvodněný „právem na bezpečnost" zaručeným článkem 6 Listiny a požadavky národní bezpečnosti (první otázka ve věcech C-511/18 a C-512/18 a třetí otázka ve věci C-511/18) a zda

– směrnice 2000/31 dovoluje uchovávání údajů, na jejichž základě lze zjistit totožnost kohokoli, kdo přispěl k vytváření obsahu dostupného veřejnosti on-line (druhá otázka ve věci C-512/18).

a) Úvodní poznámka

94. Conseil d'État (Státní rada) poukazuje na základní práva uznaná v článcích 7 (respektování soukromého a rodinného života), 8 (ochrana osobních údajů) a 11 (svoboda projevu a informací) Listiny. Jde totiž o práva, která podle Soudního dvora mohou být dotčena povinností uchovávat provozní údaje uloženou vnitrostátními orgány poskytovatelům služeb elektronických komunikací [47].

95. Předkládající soud poukazuje také na právo na bezpečnost chráněné článkem 6 Listiny. Spíše než jako o potenciálně dotčeném právu o něm hovoří jako o faktoru, jenž může odůvodnit uložení uvedené povinnosti.

46 – Body 27 až 68.

47 – Srov. rozsudek Tele2 Sverige a Watson, bod 92, v němž je obdobně odkázáno na rozsudek Digital Rights, body 25 a 70.

96. S Komisí se ztotožňuji v názoru, že odkaz na článek 6 může za těchto okolností vyznívat nejednoznačně. Stejně jako Komise mám za to, že uvedené ustanovení nelze vykládat v tom smyslu, že je způsobilé „uložit Unii pozitivní povinnost přijmout opatření k ochraně osob před trestnými činy“ [48].

97. Bezpečnost zaručená uvedeným článkem Listiny není totožná s veřejnou bezpečností. Jinými slovy, má s veřejnou bezpečností společného tolik co kterékoli jiné základní právo, protože veřejná bezpečnost je nezbytnou podmínkou k požívání základních práv a svobod.

98. Komise připomíná, že článek 6 Listiny odpovídá článku 5 Evropské úmluvy o lidských právech (dále jen „EÚLP“), jak plyne z vysvětlení k Listině. Ze znění článku 5 EÚLP plyne, že „bezpečností“ jí chráněnou je výhradně bezpečnost osobní, chápána jako záruka práva na fyzickou svobodu proti svévolnému zatčení nebo zadržení. Jde tudíž o bezpečnost spočívající v tom, že nikdo nesmí být zbaven svobody, ledaže k tomu dojde v zákonem stanovených případech a v souladu se zákonem stanovenými požadavky a postupy.

99. Jedná se proto o *osobní bezpečnost*, jež souvisí s podmínkami, za kterých lze omezit fyzickou svobodu osob [49], a nikoli o *veřejnou bezpečnost*, která se pojí s existencí státu a která je ve vyspělé společnosti nezbytným předpokladem pro nalezení rovnováhy mezi výkonem veřejné moci a požíváním individuálních práv.

100. Některé vlády nicméně požadují, aby právo na bezpečnost bylo ve větší míře zohledňováno ve druhém z uvedených významů. Soudní dvůr tyto požadavky neoslyšel, ba dokonce se o nich výslovně zmínil ve svých rozsudcích [50] a posudcích [51]. Nikdy nepopíral význam cílů obecného zájmu ochrany národní bezpečnosti a veřejného pořádku [52], boje proti mezinárodnímu terorismu za účelem zachování mezinárodního míru a bezpečnosti a boje proti závažné trestné činnosti s cílem zajistit veřejnou bezpečnost [53], který správně kvalifikoval jako „prvořadý“ [54]. Jak již kdysi rozhodl, „[z]ajištění veřejné bezpečnosti […] přispívá i k ochraně práv a svobod druhého“ [55].

101. Příležitosti poskytnuté těmito žádostmi o rozhodnutí o předběžné otázce by bylo možné využít k jednoznačnější pobídce hledat rovnováhu mezi právem na bezpečnost na jedné straně a právem na soukromí a na ochranu osobních údajů na straně druhé. Umožnilo by to vyhnout se výtkám vůči upřednostňování na druhém místě zmíněných práv na úkor prvně zmíněného práva.

102. Na tuto rovnováhu dle mého názoru odkazují bod 11 odůvodnění a čl. 15 odst. 1 směrnice 2002/58, když hovoří o požadavcích nezbytnosti a přiměřenosti opatření v *demokratické společnosti*. Právo na bezpečnost je, opakuji, nedílnou součástí samotné existence a přežití demokracie, v důsledku čehož musí být při hodnocení zmíněné přiměřenosti plně zohledněno. Jinými slovy, ačkoli je dodržení zásady důvěrnosti údajů prvořadé v demokratické společnosti, nelze podceňovat ani význam její bezpečnosti.

48 – Bod 37 písemného vyjádření Komise.

49 – Takový je výklad ESLP. Za všechny viz rozsudek ze dne 5. července 2016, Buzadji v. Moldávie, ECHR:2016:0705JUD002375507, v jehož bodě 84 se uvádí, že základním účelem práva uznaného článkem 5 EÚLP je zabraňovat svévolným nebo neodůvodněným zbavením osobní svobody.

50 – Rozsudek Digital Rights, bod 42.

51 – Posudek 1/15 (Dohoda PNR mezi EU a Kanadou), ze dne 26. července 2017 (dále jen „posudek 1/15“, EU:C:2017:592), bod 149 a citovaná judikatura.

52 – Rozsudek ze dne 15. února 2016, N. (C-601/15 PPU, EU:C:2016:84, bod 53).

53 – Rozsudek Digital Rights, bod 42 a citovaná judikatura.

54 – Tamtéž, bod 51.

55 – Posudek 1/15, bod 149.

103. Kontext vážného a trvajícího ohrožení národní bezpečnosti, a zejména rizika terorismu proto nelze – v souladu s poslední větou bodu 119 rozsudku Tele2 Sverige a Watson – pominout. Vnitrostátní systém může reagovat úměrně povaze a intenzitě hrozeb, kterým čelí, přičemž tato reakce nemusí nutně být stejná jako reakce jiných členských států.

104. Konečně musím dodat, že shora rozvedené úvahy nebrání tomu, aby v situacích skutečně výjimečných, charakterizovaných bezprostřední hrozbou nebo mimořádným rizikem, které by odůvodňovaly oficiální vyhlášení stavu nouze v členském státě, vnitrostátní předpisy obsahovaly možnost uložit na omezenou dobu povinnost uchovávat údaje natolik obecnou a tak širokého rozsahu, jak by bylo nezbytně nutné [56].

105. První otázka z obou žádostí o rozhodnutí o předběžné otázce by tudíž měla být přeformulována tak, aby byla zaměřena spíše na možnost odůvodnit zásah důvody národní bezpečnosti. Pochybnosti by se pak týkaly otázky, zda je povinnost uložená provozovatelům služeb elektronických komunikací slučitelná s čl. 15 odst. 1 směrnice 2002/58.

b) Posouzení

1) Charakteristika vnitrostátních předpisů uvedených v obou žádostech o rozhodnutí o předběžné otázce vzhledem k judikatuře Soudního dvora

106. Podle předkládacích usnesení ukládá právní úprava sporná v původních řízeních povinnost uchovávat údaje:

– provozovatelům elektronických komunikací, a sice konkrétně těm, kteří nabízejí veřejnosti on-line přístup ke komunikačním službám, a

– fyzickým či právnickým osobám, které i bezúplatně nabízejí veřejnosti on-line ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb [57].

107. Provozovatelé mají povinnost uchovávat informace umožňující identifikovat uživatele, údaje o použitých koncových komunikačních zařízeních, technické charakteristiky, datum, čas a délku trvání každého volání, údaje o vyžádaných nebo využívaných doplňkových službách a jejích poskytovatelích, jakož i údaje umožňující zjistit totožnost adresáta sdělení a v případě poskytování telefonních služeb také údaje umožňující identifikovat zdroj a lokalizaci komunikace, a to po dobu jednoho roku ode dne, kdy byly tyto informace zaznamenány [58].

108. Co se konkrétně týče služeb přístupu k internetu a služeb souvisejících s ukládáním, vnitrostátní právní úprava podle všeho vyžaduje uchovávání adres IP [59], přístupových hesel a v případě, že byla podepsána smlouva nebo otevřen platební účet, druhu provedené platby a její reference, částky, data a času transakce [60].

56 – Viz body 105 až 107 mého stanoviska ve věci C-520/18.

57 – Plyne to z článku L. 851-1 zákoníku vnitřní bezpečnosti, jenž odkazuje na článek L. 34-1 zákoníku poštovních služeb a elektronických komunikací a na článek 6 zákona č. 2004-575, o posílení důvěry v digitální ekonomiku.

58 – Tak stanoví článek R. 10-13 zákoníku poštovních služeb a elektronických komunikací.

59 – Ověření této otázky, ohledně které vyšla na jednání najevo neshoda, přísluší předkládajícímu soudu.

60 – Článek 1 nařízení vlády č. 2011-219.

109. Povinnost tohoto uchovávání je uložena s ohledem na vyšetřování, odhalování a stíhání trestných činů [61]. To znamená, že na rozdíl od povinnosti – jak bude popsáno níže – *sbírat* provozní a lokalizační údaje, není jediným cílem povinnosti *uchovávat je* předcházení terorismu [62].

110. K podmínkám *přístupu* k uchovávaným údajům je třeba uvést, že z informací poskytnutých v usnesení vyplývá, že ty jsou buď stanoveny v rámci obecného režimu (zapojení justičního orgánu), anebo je takový přístup omezen na individuálně určené a předchozím povolením předsedy vlády vydaným na základě nezávazného stanoviska nezávislého správního orgánu zmocněné činitele [63].

111. Snadno si lze všimnout, jak podotkla Komise [64], že údaje, jejichž uchovávání vyžadují vnitrostátní předpisy, odpovídají v podstatě údajům, kterými se Soudní dvůr zabýval v rozsudku Digital Rights a v rozsudku Tele2 Sverige a Watson [65]. Stejně jako tehdy se i na tyto údaje vztahuje „povinnost plošného a nerozlišujícího uchovávání“, jak zcela nepokrytě uvádí Conseil d'État (Státní rada) v úvodu svých předběžných otázek.

112. Je-li tomu tak, což musí v konečném důsledku posoudit předkládající soud, nelze než uzavřít, že dotčená právní úprava představuje „zásah[…] do základních práv zakotvených v článcích 7 a 8 Listiny, který se jeví jako rozsáhlý a musí být považován za zvlášť závažný“ [66].

113. Žádný z vyjádřivších se účastníků řízení nezpochybnil, že právní úprava s těmito charakteristikami znamená zásah do uvedených práv. Touto otázkou není nutné se dále zabývat, a to ani k připomenutí, že narušení těchto práv nevyhnutelně poškozuje samotné základy společnosti, která vedle jiných hodnot usiluje o respektování soukromého života osob chráněného Listinou.

114. Uplatnění judikatury zavedené v rozsudku Tele2 Sverige a Watson a potvrzené v rozsudku Ministerio Fiscal by přirozeně vedlo k závěru, že taková právní úprava, jako je úprava sporná v projednávaných věcech, „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, 11 a čl. 52 odst. 1 Listiny“ [67].

115. Stejně jako právní úprava posuzovaná v rozsudku Tele2 Sverige a Watson se totiž i právní úprava dotčená v projednávaných věcech „vztahuje obecně na všechny účastníky a registrované uživatele a týká se všech prostředků elektronické komunikace a veškerých provozních údajů, [přičemž] neupravuje žádné rozlišení, omezení nebo výjimky činěné v závislosti na sledovaném cíli“ [68]. „Vztahuje se tedy i na osoby, v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset se závažnou trestnou činností“, a nestanoví přitom žádnou výjimku, „takže se vztahuje i na osoby, jejichž sdělení jsou podle pravidel vnitrostátního práva předmětem profesního tajemství“ [69].

61 – Článek R. 10-13 zákoníku poštovních služeb a elektronických komunikací.

62 – La Quadrature du Net i Fédération des founisseurs d'accès à Internet associatifs poukazují na širokou škálu účelů, k nimž slouží uchovávání, diskreční pravomoc orgánů, neexistenci objektivních kritérií pro jejich vymezení a na význam přiznávaný formám trestné činnosti, které nelze kvalifikovat jako závažné.

63 – Commission nationale de contrôle des techniques de renseignement (Národní komise pro kontrolu zpravodajských metod). V tomto ohledu viz body 145 až 148 písemného vyjádření francouzské vlády.

64 – Bod 60 písemného vyjádření Komise.

65 – Ve skutečnosti jsou požadavky o něco málo vyšší, neboť v případě služeb přístupu k internetu vyžadují podle všeho také uchovávání adresy IP či přístupových hesel.

66 – Rozsudek Tele2 Sverige a Watson, bod 100.

67 – Tamtéž, bod 107.

68 – Tamtéž, bod 105.

69 – Tamtéž.

116. Sporná právní úprava dále také „nevyžaduje souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti. Zejména se 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 trestné činnosti“ [70].

117. Z výše uvedeného vyplývá, že taková právní úprava „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, 11 a čl. 52 odst. 1 Listiny“ [71].

118. Výše uvedené postačilo Soudnímu dvoru pro závěr, že příslušná ustanovení vnitrostátního práva nejsou slučitelná s čl. 15 odst. 1 směrnice 2002/58, pokud „za účelem boje proti trestné činnosti stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace“ [72].

119. Na tomto místě vyvstává otázka, zda lze judikaturu Soudního dvora v oblasti uchovávání osobních údajů ne-li změnit, tak alespoň zmírnit, když účelem tohoto „plošného a nerozlišujícího“ uchovávání je boj proti terorismu. První otázka ve věci C-511/18 byla totiž položena právě „v kontextu vážného a trvajícího ohrožení národní bezpečnosti a zejména rizika terorismu“.

120. Je nicméně třeba poznamenat, že i když povinnost uchovávat údaje byla uložena v tomto *faktickém kontextu*, její *normativní kontext* se nevztahuje jen na terorismus. Režim uchovávání údajů a přístupu k nim dotčený v řízení před Conseil d'État (Státní rada) váže uvedenou povinnost obecně na účely vyšetřování, odhalování a stíhání trestných činů.

121. V každém případě je třeba poznamenat, že argumentace obsažená v rozsudku Tele2 Sverige a Watson se vztahuje i na boj proti terorismu, a že Soudní dvůr tehdy neuvažoval o tom, že by tento druh trestné činnosti mohl někdy vyžadovat změnu jeho judikatury [73].

122. Mám proto v zásadě za to, že na otázku předkládajícího soudu soustředěnou na specifičnost hrozby terorismu by se mělo odpovědět ve stejném smyslu, v jakém Soudní dvůr rozhodl v rozsudku Tele2 Sverige a Watson.

123. Jak jsem již uvedl ve stanovisku ve věci Stichting Brein, „[n]ezavazuje-li nutnost přesného uplatňování práva soudy k tomu, aby striktně vycházely ze zásady *stare decisis*, zcela jistě je nutí alespoň k tomu, aby se pečlivě řídily svým vlastním řešením určitého právního problému, pro něž se po zralé úvaze samy rozhodly“ [74].

2) Omezené uchovávání údajů v případě hrozeb pro bezpečnost státu včetně hrozby terorismu

124. Bylo by nicméně možné upřesnit či doplnit tuto judikaturu s ohledem její na důsledky pro boj proti terorismu či pro ochranu státu před podobnými hrozbami pro národní bezpečnost?

70 – Rozsudek Tele2 Sverige a Watson, bod 106.

71 – Tamtéž, bod 107.

72 – Tamtéž, bod 112.

73 – Tamtéž, bod 103.

74 – Věc C-527/15 (EU:C:2016:938, bod 41).

125. Shora jsem již zdůraznil, že již pouhé uchovávání osobních údajů představuje zásah do práv zaručených články 7, 8 a 11 Listiny [75]. Bez ohledu na to, že jeho konečným účelem je umožnit zpětně nebo současně *přístup* k údajům v určitém okamžiku [76], představuje již pouhé uchovávání údajů nad rámec údajů naprosto nezbytných pro přenos sdělení nebo pro účtování služeb poskytovaných poskytovatelem překročení mezí stanovených články 5 a 6 směrnice 2002/58.

126. Uživatelé těchto služeb (ve skutečnosti téměř všichni občané žijící ve vyspělých společnostech) mají, resp. by měli mít, legitimní očekávání, že bez jejich souhlasu není uchováváno více jejich údajů, než které jsou ukládány v souladu s uvedenými ustanoveními. Z toho je třeba vycházet při výkladu výjimek podle čl. 15 odst. 1 směrnice 2002/58.

127. Jak jsem již vysvětlil, Soudní dvůr v rozsudku Tele2 Sverige a Watson odmítl plošné a nerozlišující uchovávání osobních údajů, a to i v souvislosti s bojem proti terorismu [77].

128. Navzdory kritice judikatury zavedené tímto rozsudkem si nemyslím, že by v ní byla podceněna hrozba terorismu coby forma obzvláště závažné trestné činnosti, jejímž jednoznačným cílem je reakce vůči autoritě státu a destabilizace či destrukce jeho institucí. Boj proti terorismu je pro stát doslova životně důležitý a úspěch tohoto boje je cílem obecného zájmu, na který právní stát nemůže rezignovat.

129. Prakticky všechny vlády zúčastněné na řízení se i s Komisí shodly na tom, že vedle technických obtíží by částečné a rozlišující uchovávání osobních údajů zbavilo vnitrostátní zpravodajské služby možnosti získat přístup k informacím nezbytným pro identifikaci hrozeb pro veřejnou bezpečnost a obranu státu, jakož i pro stíhání pachatelů teroristických útoků [78].

130. K tomuto názoru považuji za potřebné podotknout, že na boj proti terorismu nelze nahlížet jen z hlediska jeho účinnosti. Proto je tak složitý, ale i tak působivý, když jeho prostředky a metody odpovídají požadavkům právního státu, tedy především podřízení moci a síly omezením práva, a zejména právnímu řádu, který si obranu základních práv vytyčil jako smysl a cíl své existence.

131. Jestliže z pohledu terorismu světí jeho prostředky jen ryzí (a co nejvyšší) účinnost jeho útoků na zavedený řád, právní stát měří efektivitu způsobem, který nepřipouští, aby se při jeho obraně upustilo od postupů a záruk, které jej kvalifikují jako řád legitimní. Kdyby se právní stát oddal bez dalšího pouhé efektivitě, ztratil by svou charakteristickou vlastnost a sám by se v krajních případech mohl stát hrozbou pro občana. Nijak by nebylo možné zajistit, že když veřejná moc bude vybavena nadměrně nepřiměřenými nástroji pro stíhání trestných činů, díky nimž bude moci ignorovat nebo porušovat základní práva, neobrátí se její nekontrolované a naprosto volné působení proti svobodě všech.

75 – Jak připomněl již Soudní dvůr v posudku 1/15, bod 124, „sdělování osobních údajů třetí straně, například veřejnému orgánu, je zásahem do základního práva zakotveného v článku 7 Listiny, bez ohledu na následné využití sdělených informací. Totéž platí pro uchovávání osobních údajů a pro jejich zpřístupňování za účelem jejich využití veřejnými orgány. V tomto ohledu není důležité, zda dotyčné informace o soukromém životě představují citlivé údaje nebo zda dotyčné osoby utrpěly z důvodu tohoto zásahu případné nepříznivé následky“.

76 – Jak uvedl generální advokát P. Cruz Villalón ve svém stanovisku ve věci Digital Rights, C-293/12 a C-594/12 (EU:C:2013:845, bod 72), „shromažďování a především uchovávání – v enormních databázích – mnoha údajů vytvářených či zpracovávaných v rámci velké části běžné elektronické komunikace občanů Unie představuje závažný zásah do jejich soukromého života, i když jen vytvářejí podmínky pro možnost zpětně kontrolovat jejich osobní i profesní aktivity. Shromažďování těchto údajů vytváří podmínky pro sledování, které i přesto, že k němu dochází jen zpětně při jejich využívání, představuje pro právo občanů Unie na utajení jejich soukromého života permanentní hrozbu trvající po celou dobu uchovávání oněch údajů. Vzniklý dojem jakéhosi sledování vyvolává velmi intenzivně otázku doby uchovávání údajů.“

77 – Rozsudek Tele2 Sverige a Watson, bod 103: „nemůže […] odůvodnit, že vnitrostátní právní úprava, která stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů, je považována za nezbytnou pro účely uvedeného boje“.

78 – Takový výklad hájí například francouzská vláda, která tento argument názorně dokládá konkrétními příklady užitečnosti plošného uchovávání údajů, jež státu umožnilo reagovat na závažné teroristické útoky, ke kterým v její zemi došlo v posledních letech (body 107 a 122 až 126 písemného vyjádření francouzské vlády).

132. Nepřekonatelnou hranicí efektivity veřejné moci jsou, opakuji, základní práva občanů, jejichž omezení lze zavést, jak stanoví čl. 52 odst. 1 Listiny, pouze zákonem – přičemž musí být respektována podstata těchto práv – a tehdy, „jsou-li nezbytná a skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého“ [79].

133. K podmínkám, za kterých by podle rozsudku Tele2 Sverige a Watson bylo přípustné *cílené* uchovávání údajů, se vyjadřuji ve svém stanovisku ve věci C-520/18 [80].

134. Situace, kdy lze na základě dostupných informací v rukou bezpečnostních služeb potvrdit důvodné podezření z přípravy teroristického útoku, může být legitimním předpokladem pro uložení povinnosti uchovávat určité údaje. Tím spíše jím může být skutečné spáchání útoku. Pokud v posledně zmíněném případě může spáchání trestného činu samo o sobě představovat faktor odůvodňující přijetí řečeného opatření, v případě pouhého podezření na případný útok by bylo nezbytné, aby okolnosti, které toto podezření dokládají, vykazovaly určitou minimální míru věrohodnosti, jež je nezbytná pro objektivní vážení indicií, které jsou způsobilé jej doložit.

135. Přestože je to náročné, není nemožné přesně a v souladu s objektivními kritérii určit jak kategorie údajů, jejichž uchovávání se jeví jako nezbytné, tak i okruh dotčených osob. *Nejpraktičtější a nejúčinnější* by zajisté bylo plošné a nerozlišující uchovávání všech údajů, které by poskytovatelé služeb elektronických komunikací mohli vůbec získat, avšak již jsem předeslal, že otázku nelze řešit s ohledem na *praktickou efektivitu*, nýbrž s ohledem na *právní efektivitu* a v kontextu právního státu.

136. Toto určení je typicky úlohou zákonodárce, a to v rámci mezí vytyčených judikaturou Soudního dvora. Znovu odkazuji na úvahy, které k této problematice rozvádím ve stanovisku ve věci C-520/18 [81].

3) Přístup k uchovávaným údajům

137. Za předpokladu, že poskytovatelé při sběru údajů dodrželi ustanovení směrnice 2002/58 a k uchovávání těchto údajů docházelo v souladu s čl. 15 odst. 1 [82], musí přístup příslušných orgánů k těmto informacím probíhat v souladu s podmínkami vyžadovanými Soudním dvorem, které analyzuji ve stanovisku ve věci C-520/18, na něž odkazuji [83].

138. Proto i v tomto případě musí vnitrostátní právní úprava stanovit hmotněprávní a procesní podmínky upravující přístup příslušných orgánů k uchovávaným údajům [84]. V kontextu projednávaných žádostí o rozhodnutí o předběžné otázce by tyto podmínky dovolovaly přístup k údajům osob, u nichž je podezření, že připravují, páchají či spáchaly teroristický útok nebo se na něm mohly podílet [85].

79 – Rozsudek ze dne 15. února 2016, N. (C-601/15 PPU, EU:C:2016:84, bod 50). Jde tedy o křehkou rovnováhu mezi veřejným pořádkem a svobodou, o které jsem již hovořil a která je zásadně metou celého unijního právního řádu. Příkladmo lze uvést směrnici Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV (Úř. věst. 2017, L 88, s. 6). Zatímco v čl. 20 odst. 1 je členským státům uložena povinnost zajistit, aby osoby, útvary nebo služby příslušné k vyšetřování nebo stíhání trestných činů terorismu „měly k dispozici účinné vyšetřovací nástroje“, v bodě 21 jejího odůvodnění se uvádí, že používání těchto účinných nástrojů „by mělo být cílené a je při něm třeba zohledňovat zásadu proporcionality a povahu a závažnost vyšetřovaných trestných činů a dodržovat právo na ochranu osobních údajů“.

80 – Body 87 až 95.

81 – Body 100 až 107.

82 – Přičemž jsou dodrženy podmínky uvedené v bodě 122 rozsudku Tele2 Sverige a Watson, v němž Soudní dvůr připomněl, že čl. 15 odst. 1 směrnice 2002/58 nepřipouští odchylky od jejího čl. 4 odst. 1 a 1a, na jejichž základě mají poskytovatelé povinnost přijmout opatření, která umožní zajistit ochranu uchovávaných údajů proti riziku zneužití a proti jakémukoli neoprávněnému přístupu. V této souvislosti uvedl, že „[v]zhledem k množství uchovávaných údajů, jejich citlivé povaze a riziku neoprávněného přistupování k nim musí poskytovatelé služeb elektronických komunikací v zájmu zajištění plné integrity a důvěrné povahy těchto údajů zaručit vhodnými technickými a organizačními opatřeními mimořádně vysokou úroveň ochrany a bezpečnosti. Vnitrostátní právní úprava musí zejména stanovit, že údaje musí být uchovávány na území Unie a že po uplynutí lhůty pro jejich uchovávání musí dojít k jejich nevratné likvidaci“.

83 – Body 52 až 60.

84 – Rozsudek Tele2 Sverige a Watson, bod 118.

85 – Tamtéž, bod 119.

139. Zásadní ovšem je, aby přístup k dotčeným údajům – s výjimkou řádně odůvodněných naléhavých případů – podléhal předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu, které rozhodnou na základě odůvodněné žádosti příslušných orgánů [86]. Tam, kam nemůže dosáhnout abstraktní posouzení zákonodárce, je tak zaručeno konkrétní posouzení tohoto nezávislého orgánu, jenž musí stejnou měrou zajistit bezpečnost státu i ochranu základních práv občanů.

4) Povinnost uchovávat údaje umožňující zjistit totožnost tvůrců obsahu s ohledem na směrnici 2000/31 (druhá předběžná otázka ve věci C-512/18)

140. Předkládající soud odkazuje na směrnici 2000/31 jakožto na referenční bod při rozhodování, zda je možné určitým osobám [87] a provozovatelům nabízejícím komunikační služby veřejnosti uložit 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 soudní orgán v případě potřeby požadovat informace s cílem zajistit dodržování pravidel týkajících se občanskoprávní nebo trestněprávní odpovědnosti“.

141. S Komisí se ztotožňuji v názoru, že není namístě zkoumat slučitelnost této povinnosti se směrnicí 2000/31 [88], neboť její čl. 1 odst. 5 písm. b) vylučuje z oblasti její působnosti „otázky týkající se služeb informační společnosti upravené ve směrnicích 95/46/ES a 97/66/ES“, tedy v předpisech, jimž v současné době odpovídá nařízení 2006/679 a směrnice 2002/58 [89], přičemž čl. 23 odst. 1 nařízení 2006/679 a čl. 15 odst. 1 směrnice 2002/58 je podle mého názoru třeba vykládat shora rozvedeným způsobem.

2. K povinnosti sbírat provozní a lokalizační údaje v reálném čase (druhá předběžná otázka ve věci C-511/18)

142. Ustanovení článku L. 851-2 zákoníku vnitřní bezpečnosti podle předkládajícího soudu umožňují výhradně pro účely předcházení terorismu sbírat v reálném čase informace o osobách dříve identifikovaných jako podezřelé z vazeb na hrozbu terorismu. Stejně tak článek L. 851-4 téhož zákoníku umožňuje, aby provozovatelé v reálném čase předávali technické údaje o poloze koncových zařízení.

143. Podle předkládajícího soudu neukládají tyto metody poskytovatelům služeb povinnost dalšího uchovávání vedle toho, které je nezbytné pro účtování a prodej jejich služeb.

144. Podle článku L. 851-3 zákoníku vnitřní bezpečnosti lze navíc provozovatelům elektronických komunikací a poskytovatelům technických služeb uložit povinnost „na svých sítích […] na základě parametrů uvedených v povolení zavést automatizované procesy za účelem odhalování spojení, která by mohla ukazovat na hrozbu terorismu“. Tato metoda nezahrnuje plošné a nerozlišující uchovávání údajů a jejím účelem je po omezenou dobu sbírat ty údaje o připojení, které by mohly mít souvislost s teroristickou trestnou činností.

145. Mám za to, že i na přístup k údajům vytvářeným v průběhu elektronických komunikací v reálném čase se musí uplatnit podmínky platné pro přístup k uchovávaným osobním údajům. V tomto konkrétním ohledu tedy odkazuji na výše rozvedené úvahy. Nezáleží na tom, zda jde o uchovávané, nebo o bezprostředně získané údaje, neboť v obou případech dochází k seznámení se s osobními údaji, ať již jde o údaje starší, nebo aktuální.

86 – Tamtéž, bod 120.

87 – A sice těm, které „nabízejí veřejnosti služby veřejné komunikace on-line, ukládání znaků, dokumentů, obrázků, zvuků nebo zpráv jakékoli povahy poskytnutých příjemci těchto služeb […]“.

88 – Tuto směrnici velmi obecně a bez odkazu na jakékoli konkrétní ustanovení zmiňuje předkládající soud ve druhé otázce ve věci C-512/18.

89 – Bod 112 a 113 písemného vyjádření Komise.

146. Konkrétně kdyby přístup v reálném čase byl důsledkem připojení odhalených za pomoci automatizovaných procesů, jak se uvádí v článku L. 851-3 zákoníku vnitřní bezpečnosti, pak vzorce a kritéria předem stanovené pro tyto procesy musí být specifické, spolehlivé a nediskriminační, aby umožnily identifikovat jednotlivce, u kterých existuje důvodné podezření z podílení se na teroristických činnostech [90].

3. K povinnosti vyrozumět dotčené osoby (třetí předběžná otázka ve věci C-511/18)

147. Soudní dvůr již rozhodl, že orgány, jimž byl poskytnut přístup k údajům, mají o tomto přístupu vyrozumět dotčené osoby, pokud tím nebude ohroženo probíhající vyšetřování. Důvodem této povinnosti je, že toto vyrozumění je nezbytné k tomu, aby tyto osoby mohly v případě, že byla porušena jejich práva, uplatnit své právo na účinnou právní ochranu výslovně zmíněné v čl. 15 odst. 2 směrnice 2002/58 [91].

148. Conseil d'État (Státní rada) se v rámci své třetí otázky ve věci C-511/18 táže, zda je taková informační povinnost nevyhnutelná v každém případě, nebo zda lze od ní upustit, když jsou stanoveny jiné záruky, jako například záruky popsané v jejím předkládacím usnesení.

149. Předkládající soud popisuje [92], že uvedené záruky spočívají v možnosti každého, kdo má zájem si ověřit případnou protiprávnost uplatnění určité zpravodajské metody, se obrátit na samotnou Conseil d'État (Státní rada). Tento orgán má pak možnost případně zrušit povolení takového opatření a nařídit likvidaci sesbíraného materiálu, a to v řízení, ve kterém neplatí zásada kontradiktornosti obvyklá v soudních řízeních.

150. Předkládající soud má za to, že tato právní úprava není v rozporu s právem na účinnou právní ochranu. Já se ovšem domnívám, že uvedené by bylo možno teoreticky připustit v případě osob, které chtějí zjistit, zda nejsou předmětem zpravodajské operace. Naproti tomu toto právo není dodrženo tehdy, pokud osoby, které jsou nebo byly předmětem takové operace, nebyly o této skutečnosti vyrozuměny, a tudíž nemohou ani jen uvažovat o tom, zda jejich práva byla či nebyla porušena.

151. Soudní záruky, na které poukazuje předkládající soud, jsou podle všeho závislé na iniciativě toho, kdo má podezření, že je předmětem sběru informací o své osobě. Přístup k soudu za účelem ochrany svých práv musí ovšem platit pro všechny, z čehož plyne, že každý, jehož osobní údaje byly zpracovávány, musí mít možnost před soudem zpochybnit legalitu tohoto zpracovávání, které mu tudíž musí být oznámeno.

152. Soud sice může, jak plyne z poskytnutých informací, zahájit řízení i bez návrhu nebo na základě správní stížnosti, avšak dotčené osobě musí být v každém případě umožněno, aby sama zahájila takové řízení, k čemuž je nezbytné, aby byla vyrozuměna o tom, že její osobní údaje byly zpracovávány určitým způsobem. Pro účely ochrany jejích práv nelze spoléhat na to, že se o tomto zpracovávání dozví od třetích osob nebo vlastními prostředky.

153. Pokud není ohroženo probíhající vyšetřování, pro jehož účely byl poskytnut přístup k uchovávaným údajům, musí tedy být dotčená osoba o tomto přístupu vyrozuměna.

90 – Rozsudek Digital Rights, bod 59.

91 – Rozsudek Tele2 Sverige a Watson, bod 121.

92 – Body 8 až 11 předkládacího usnesení.

154. Jinou otázkou je nutnost, aby soudní řízení vedené na návrh dotčené osoby podaný poté, co byla obeznámena s přístupem ke svým údajům, odpovídalo požadavkům důvěrnosti a opatrnosti nezbytným při kontrole zákonnosti postupu orgánů veřejné moci v takových citlivých oblastech, jako je bezpečnost a obrana státu. Této otázky se ovšem projednávané žádosti o rozhodnutí o předběžné otázce netýkají, takže podle mého názoru není namístě, aby o ní Soudní dvůr rozhodoval.

V. Závěry

155. S ohledem na výše uvedené navrhuji, aby Soudní dvůr na otázky Conseil d'État (Státní rada, Francie) odpověděl takto:

„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 spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie musí být vykládán v tom smyslu, že:

1) brání takové vnitrostátní právní úpravě, která v kontextu vážného a trvajícího ohrožení národní bezpečnosti, a zejména rizika terorismu ukládá provozovatelům a poskytovatelům služeb elektronických komunikací povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků, jakož i údaje umožňující zjistit totožnost tvůrců obsahu nabízeného poskytovateli uvedených služeb;

2) brání takové vnitrostátní právní úpravě, která nezavádí povinnost vyrozumět dotčené osoby o zpracování jejich osobních údajů prováděném příslušnými orgány, ledaže by takové vyrozumění ohrozilo činnost těchto orgánů;

3) nebrání takové vnitrostátní právní úpravě, která umožňuje sbírat v reálném čase provozní a lokalizační údaje konkrétních jednotlivců, pokud k takovému sběru dochází v souladu s postupy stanovenými pro přístup k legitimně uchovávaným osobním údajům a se stejnými zárukami.“