Sbírka soudních rozhodnutí

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

Věc C-520/18

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

[žádost o rozhodnutí o předběžné otázce podaná Cour constitutionnelle (Ústavní soud, Belgie)]

„Řízení o předběžné otázce – Zpracovávání osobních údajů a ochrana soukromí v odvětví elektronických komunikací – Směrnice 2002/58/ES – Oblast působnosti – Článek 1 odst. 3 – Článek 15 odst. 1 – Článek 4 odst. 2 SEU – Listina základních práv Evropské unie – Články 4, 6, 7, 8, 11 a 52 odst. 1 – Povinnost plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů – Účinnost vyšetřování trestných činů a další cíle veřejného zájmu“

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;

[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).

– 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];

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

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 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.

5. Po vyhlášení rozsudku Digital Rights zrušil Cour constitutionnelle (Ústavní soud, Belgie) vnitrostátní právní úpravu, která částečně provedla do vnitrostátního práva směrnici 2006/24, jež byla tímto rozsudkem prohlášena za neplatnou. Belgický zákonodárce tedy přijal novou právní úpravu, o jejíž slučitelnosti s unijním právem vznikly v důsledku rozsudku Tele2 Sverige a Watson pochybnosti.

6. Specifičnost této žádosti o rozhodnutí o předběžné otázce spočívá v tom, že vyvstává možnost prodloužit dočasně účinky vnitrostátního předpisu, který musí být vnitrostátními soudy zrušen pro neslučitelnost s unijním právem.

I. Právní rámec

A. Unijní právo

7. Odkazuji na příslušný bod svého stanoviska ve věcech C-511/18 a C-512/18.

[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).

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

[7] – Kromě projednávané věci (C-520/18, Ordre des barreaux francophones et germanophone a další) se jedná o věci C-511/18 a C-512/18, La Quadrature du Net a další, a C-623/17, Privacy International.

[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.

B. Vnitrostátní právo. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Článek 4 stanoví, že článek 126 loi du 13 juin 2005 relative aux communications électroniques [12] zní takto:

„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.

[…]

2. Pouze následující orgány mohou na žádost získat od poskytovatelů nebo provozovatelů uvedených v odstavci 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 článcích 46 *bis* a 88 *bis* Code d'instruction criminelle (trestní řád) a za podmínek v nich stanovených;

2) zpravodajské a bezpečnostní služby za účelem plnění zpravodajských úkolů za použití metod sběru údajů uvedených v článcích 16/2, 18/7 a 18/8 loi du 30 novembre 1998 organique des services de renseignement et de Sécurité[13] 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)] za účelem odhalování, vyšetřování a stíhání porušení [pravidel o bezpečnosti sítí] 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 […] 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 Jednotky pro pohřešované osoby Federální policie 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

[11] – Zákon ze dne 29. května 2016 o sběru a uchovávání údajů v oblasti elektronických komunikací; dále jen „zákon ze dne 29. května 2016" (Moniteur belge ze dne 18. července 2016, s. 44717).

[12] – Zákon ze dne 13. června 2005 o elektronických komunikacích; dále jen „zákon z roku 2005" (*Moniteur belge* ze dne 20. června 2005, s. 28070).

[13] – Organický zákon ze dne 30. listopadu 1998 o zpravodajských a bezpečnostních službách; dále jen „zákon z roku 1998" (*Moniteur belge* ze dne 18. prosince 1998, s. 40312).

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

6) mediační služba pro telekomunikace za účelem zjištění totožnosti osoby, která využila síť nebo službu elektronických komunikací zlovolně […]. Lze žádat pouze o identifikační údaje.

Poskytovatelé a provozovatelé uvedení v odstavci 1 prvním pododstavci zajistí, aby byly údaje uvedené v odstavci 3 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 [příslušného] ministra a po konzultaci s Komisí pro ochranu soukromí a s Institutem stanoví druhy údajů dle kategorií uvedených v prvním až třetím pododstavci, které mají být uchovávány, a požadavky, které musí tyto údaje splňovat.

4. Za účelem uchovávání údajů uvedených v odstavci 3 poskytovatelé a provozovatelé uvedení v odstavci 1 prvním pododstavci:

1) zajistí, aby měly uchovávané údaje stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně jako údaje na síti;

2) zajistí, aby se na uchovávané údaje vztahovala vhodná technická a organizační opatření k jejich ochraně před náhodným nebo neoprávněným zničením, náhodnou ztrátou či pozměněním nebo nepovoleným nebo neoprávněným uchováním, zpracováním, přístupem nebo zveřejněním;

3) zajistí, aby měl k údajům uchovávaným za účelem odpovídání na žádosti orgánů uvedených v odstavci 2 přístup pouze jeden nebo několik příslušníků koordinační jednotky uvedené v článek 126/1 odst. 1;

4) uchovají údaje na území Evropské unie;

5) zavedou technická ochranná opatření, která zajistí, aby nebyly uchovávané údaje od svého zaznamenání čitelné a použitelné nikým, kdo není zmocněn k přístupu k nim;

6) zničí uchovávané údaje na všech nosičích na konci doby uchování použitelné na tyto údaje, která je stanovena v odstavci 3, aniž jsou dotčeny články 122 a 123;

7) zajistí sledovatelnost využití uchovaných údajů u každé žádosti o poskytnutí těchto údajů ze strany orgánu uvedeného v odstavci 2.

Sledovatelnost stanovená v prvním pododstavci bodě 7 je zajištěna prostřednictvím deníku. Institut a Komise pro ochranu soukromí mohou do tohoto deníku nahlédnout nebo si vyžádat kopii tohoto deníku nebo jeho části. Institut a Komise pro ochranu soukromí uzavřou memorandum o spolupráci ohledně sledování obsahu deníku a jeho kontroly.

5. Ministr a ministr spravedlnosti předají každoročně Poslanecké sněmovně statistiky uchovávání údajů vytvořených nebo zpracovávaných v rámci poskytování komunikačních služeb nebo sítí dostupných veřejnosti.

Tyto statistiky zahrnují zejména:

1) případy, v nichž byly údaje předány příslušným orgánům v souladu s použitelnými právními předpisy;

2) dobu, která uplynula mezi datem, od něhož byly údaje uchovávány, a datem, k němuž příslušné orgány žádaly o jejich předání;

3) případy, v nichž žádosti o údaje nebylo možné uspokojit.

Tyto statistiky nesmí zahrnovat osobní údaje.

[…]“

9. Článkem 5 byl do zákona z roku 2005 vložen článek 126/1 v tomto znění:

„1. U každého provozovatele a u každého poskytovatele uvedeného v čl. 126 odst. 1 prvním pododstavci se zřídí koordinační jednotka, která poskytuje zákonem zmocněným belgickým orgánům na jejich žádost údaje uchovávané na základě článků 122, 123 a 126, identifikační údaje volajícího na základě čl. 107 odst. 2 prvního pododstavce nebo údaje, které lze vyžadovat na základě článků 46 *bis*, 88 *bis* a 90 *ter* trestního řádu a článků 18/7, 18/8, 18/16 y 18/17 zákona [z roku 1998].

[…]

2. Každý provozovatel a každý poskytovatel uvedený v čl. 126 odst. 1 prvním pododstavci stanoví vnitřní postup umožňující odpovídat na žádosti orgánů o přístup k osobním údajům týkajícím se uživatelů. Na žádost poskytne Institutu údaje o těchto postupech, o počtu obdržených žádostí, o uplatněném právním základě a o poskytnuté odpovědi.

[…]

3. Každý poskytovatel a každý provozovatel uvedený v čl. 126 odst. 1 prvním pododstavci určí jednoho nebo několik zaměstnanců pověřených ochranou osobních údajů, kteří musí splňovat kumulativní podmínky uvedené v odst. 1 třetím pododstavci.

[…]

Zaměstnanec pověřený ochranou osobních údajů jedná při plnění svých úkolů zcela nezávisle a má přístup ke všem osobním údajům předávaným orgánům, jakož i do všech příslušných prostor daného poskytovatele nebo provozovatele.

[…]

4. Král vyhláškou schválenou Radou ministrů po konzultaci s Komisí pro ochranu soukromí a s Institutem stanoví:

[…]

2) požadavky, které musí splňovat koordinační jednotka, a to s ohledem na situaci provozovatelů a poskytovatelů, kteří dostávají nízký počet žádostí od soudních orgánů, kteří nejsou usazeni v Belgii nebo kteří vykonávají činnost převážně ze zahraničí;

3) informace, které mají být poskytnuty Institutu a Komisi pro ochranu soukromí v souladu s odstavci 1 a 3, jakož i orgány, které mají k těmto informacím přístup;

4) ostatní pravidla upravující spolupráci provozovatelů a poskytovatelů uvedených v čl. 126 odst. 1 prvním pododstavci s belgickými orgány nebo některými z nich za účelem poskytování údajů uvedených v odstavci 1, a to včetně formy a obsahu žádosti, je-li to nezbytné a s ohledem na příslušný orgán.

[…]“

10. Na základě článku 8 zní článek 46 *bis* odst. 1 trestního řádu takto:

„1. Při odhalování trestných činů může státní zástupce písemným a odůvodněným rozhodnutím, když podle potřeby požádá o součinnost provozovatele elektronické komunikační sítě nebo poskytovatele služby elektronické komunikace anebo policejní oddělení určené Králem, na základě všech údajů, které má k dispozici, nebo prostřednictvím přístupu k evidenci zákazníků, kterou vedou provozovatelé nebo poskytovatelé služeb, provést nebo nechat provést:

1) identifikaci účastníka nebo obvyklého uživatele služby elektronické komunikace nebo použitého elektronického komunikačního prostředku;

2) identifikaci služeb elektronické komunikace, jichž se určitá osoba účastní nebo které určitá osoba obvykle používá.

Z odůvodnění musí vyplývat přiměřenost ve vztahu k respektování soukromého života a podpůrná povaha ve vztahu ke všem ostatním povinnostem při vyšetřování.

V krajně naléhavých případech může každý příslušník soudní policie s předchozím ústním souhlasem státního zástupce a na základě odůvodněného a písemného rozhodnutí tyto údaje vyžádat. Příslušník soudní policie toto odůvodněné a písemné rozhodnutí, jakož i získané informace sdělí státnímu zástupci ve lhůtě dvaceti čtyř hodin a kromě toho odůvodní krajní naléhavost.

Ohledně trestných činů, za které nelze uložit hlavní trest odnětí svobody na jeden rok nebo přísnější trest, si státní zástupce nebo v případě krajní naléhavosti příslušník soudní policie může vyžádat údaje uvedené v prvním pododstavci pouze po dobu šesti měsíců před vydáním svého rozhodnutí.

2. Každý provozovatel elektronické komunikační sítě a každý poskytovatel služby elektronické komunikace, který je požádán o sdělení údajů uvedených v prvním odstavci, předá státnímu zástupci nebo příslušníkovi soudní policie požadované údaje ve lhůtě, kterou stanoví král […]

[…]

Každý, kdo vzhledem ke své funkci ví o opatření nebo v rámci opatření poskytuje součinnost, je povinen zachovávat mlčenlivost. Každé porušení této mlčenlivosti se trestá podle článku 458 Code pénal (trestní zákoník).

Za odmítnutí sdělit údaje lze uložit pokutu od dvaceti šesti eur do deseti tisíc eur.“

11. Článek 88 *bis* trestního řádu má na základě článku 9 toto znění:

„1. V případě, že existují přesvědčivé indicie, že za trestné činy lze jako hlavní uložit trest odnětí svobody na jeden rok nebo trest přísnější, a má-li vyšetřující soudce za to, že existují okolnosti, které vyžadují za účelem zjištění pravdy vyhledat elektronická sdělení nebo lokalizovat zdroj nebo adresáta elektronických sdělení, může nechat provést, když požádá podle potřeby přímo či prostřednictvím policejního oddělení určeného Králem o technickou pomoc provozovatele sítě elektronické komunikace nebo poskytovatele služby elektronické komunikace:

1) vyhledání provozních údajů elektronických komunikačních prostředků, ze kterých nebo na které jsou nebo byla elektronická sdělení zaslána;

2) lokalizaci zdroje nebo adresáta elektronického sdělení.

V případech uvedených v prvním pododstavci se pro každý elektronický komunikační prostředek, jehož údaje o hovoru se vyhledávají nebo jehož zdroj nebo adresát elektronického sdělení se lokalizují, v protokolu zaznamená den, hodina, délka trvání a v případě potřeby místo elektronického sdělení.

Vyšetřující soudce uvede v odůvodněném usnesení skutkové okolnosti věci, které odůvodňují opatření, jeho přiměřenost ve vztahu k respektování soukromého života a jeho podpůrný charakter ke všem ostatním povinnostem při vyšetřování.

Rovněž uvede dobu, po kterou se bude moci opatření uplatnit do budoucna, přičemž tato doba nesmí přesáhnout dva měsíce od usnesení, aniž je dotčeno její případné obnovení, a případně dobu, na kterou se usnesení uplatní zpětně v souladu s odstavcem 2.

[…]

2. Pokud jde o uplatnění opatření uvedeného v odst. 1 prvním pododstavci na provozní nebo lokalizační údaje uchovávané na základě článku 126 zákona […] z roku 2005 […], použijí se následující ustanovení:

– u trestného činu uvedeného v části II hlavě I *ter* trestního zákoníku si může vyšetřující soudce v usnesení vyžádat údaje za dobu dvanácti měsíců před usnesením;

– u jiných trestných činů uvedených v čl. 90 *ter* odst. 2 až 4, které nejsou uvedeny v první odrážce, u trestných činů spáchaných v rámci zločinecké skupiny podle článku 324 *bis* trestního zákoníku, nebo u trestného činu, za který lze jako hlavní uložit trest odnětí svobody na pět let nebo trest přísnější, si může vyšetřující soudce v usnesení vyžádat údaje za dobu devíti měsíců před usnesením;

– u ostatních trestných činů si vyšetřující soudce může vyžádat údaje pouze za dobu šesti měsíců před usnesením.

3. Opatření se může vztahovat na elektronické komunikační prostředky advokáta nebo lékaře pouze tehdy, je-li on sám podezřelý ze spáchání trestného činu uvedeného v odstavci 1 nebo z účasti na něm nebo nasvědčují-li konkrétní skutkové okolnosti tomu, že jiné osoby podezřelé ze spáchání trestného činu uvedeného v odstavci 1 využívají jeho elektronické komunikační prostředky.

Opatření nelze provést bez vyrozumění předsedy advokátní komory nebo zástupce provinciální lékařské komory, v závislosti na konkrétním případě. Vyšetřující soudce sdělí týmž osobám skutečnosti, na které se podle něj vztahuje profesní tajemství. Tyto skutečnosti nejsou zaznamenány v protokolu.

4. […]

Každý, kdo vzhledem ke své funkci ví o opatření nebo v rámci opatření poskytuje součinnost, je povinen zachovávat mlčenlivost. Každé porušení této mlčenlivosti se trestá podle článku 458 trestního zákoníku.

[…]“

12. Na základě článku 12 má článek 13 zákona z roku 1998 následující znění:

„Zpravodajské a bezpečnostní služby mohou vyhledávat, shromažďovat, získávat a zpracovávat informace a osobní údaje, které mohou být užitečné pro plnění jejich úkolů, a vést aktuální záznamy mimo jiné o událostech, skupinách a osobách, které jsou relevantní pro plnění jejich úkolů.

Informace obsažené v záznamech musí mít souvislost s účelem evidence a musí být omezeny na požadavky z něj vyplývající.

Zpravodajské a bezpečnostní služby zajistí bezpečnost údajů o jejich zdrojích a informací a osobních údajů poskytnutých těmito zdroji.

Příslušníci zpravodajských a bezpečnostních služeb mají přístup k informacím a osobním údajům shromažďovaným a zpracovávaným službou, ke které náleží, jsou-li užitečné při výkonu jejich povolání nebo plnění jejich úkolů.“

13. Článek 14 určuje nové znění článku 18/3, jenž nyní stanoví:

„1. Zvláštní metody sběru údajů uvedené v čl. 18/2 odst. 1 lze použít s ohledem na možnou hrozbu uvedenou v článku 18/1, jsou-li obvyklé metody sběru údajů považovány za nedostatečné k umožnění získání informací nezbytných pro dokončení zpravodajského úkolu. Zvláštní metoda musí být zvolena v závislosti na stupni závažnosti možné hrozby, ohledně které je použita.

Zvláštní metodu lze použít až po písemném a odůvodněném rozhodnutí ředitele služby a po oznámení tohoto rozhodnutí komisi.

2. V rozhodnutí ředitele služby se uvede:

1) druh zvláštní metody;

2) v závislosti na konkrétním případu fyzické nebo právnické osoby, sdružení nebo skupiny, předměty, místa, události nebo informace, na které se vztahuje zvláštní metoda;

3) možná hrozba, která odůvodňuje zvláštní metodu;

4) skutkové okolnosti, které odůvodňují zvláštní metodu, odůvodnění podpůrné povahy a přiměřenosti, a to včetně spojitosti mezi body 2 a 3;

5) doba, po kterou lze zvláštní metodu použít ode dne oznámení rozhodnutí komisi;

[…]

9) případně závažné indicie o tom, že se advokát, lékař nebo novinář osobně a aktivně podílí nebo podílel na vzniku nebo vývoji možné hrozby;

10) v případě uplatnění článku 18/8 odůvodnění délky doby shromažďování údajů;

[…]

8. Ředitel služby ukončí zvláštní metodu, pokud pominula možná hrozba, která ji odůvodňovala, pokud již metoda není užitečná s ohledem na účel, pro který byla použita, nebo pokud konstatoval protiprávnost. O svém rozhodnutí uvědomí v co nejkratší lhůtě komisi.“

14. Ustanovení článku 18/8 zákona z roku 1988 má toto znění:

„1. Zpravodajské a bezpečnostní služby mohou v zájmu plnění svých úkolů, a v případě potřeby za tímto účelem i s vyžádáním technické pomoci provozovatele sítě elektronických komunikací nebo poskytovatele služby elektronických komunikací, provést nebo nechat provést:

1) vyhledání provozních údajů elektronických komunikačních prostředků, ze kterých nebo na které jsou nebo byla elektronická sdělení zaslána;

2) lokalizaci zdroje nebo adresáta elektronických sdělení.

[…]

2. Pokud jde o použití metody uvedené v odstavci 1 na údaje uchovávané na základě článku 126 zákona […] z roku 2005 […], použijí se následující ustanovení:

1) u možné hrozby, která se vztahuje na činnost, jež může být spojena se zločineckou skupinou nebo škodlivou sektářskou organizací, si ředitel služby může v rozhodnutí vyžádat údaje pouze za dobu šesti měsíců před rozhodnutím;

2) u jiné možné hrozby, než jsou hrozby uvedené v bodech 1 a 3, si ředitel služby může v rozhodnutí vyžádat údaje za dobu devíti měsíců před rozhodnutím;

3) u možné hrozby, která se vztahuje na činnost, jež může být spojena s terorismem nebo extrémismem, si ředitel služby může v rozhodnutí vyžádat údaje za dobu dvanácti měsíců před rozhodnutím. […]“

II. Skutkové okolnosti a předběžné otázky

15. V rozsudku ze dne 11. června 2015 [14] Cour constitutionnelle (Ústavní soud) zrušil nové znění článku 126 zákona z roku 2005 z týchž důvodů, které vedly Soudní dvůr k prohlášení směrnice 2006/24 v rozsudku Digital Rights za neplatnou.

16. Vnitrostátní zákonodárce s ohledem na toto zrušení schválil (před tím, než byl vydán rozsudek Tele2 Sverige a Watson) zákon ze dne 29. května 2016.

17. VZ a další, Ordre des barreaux francophones et germanophone („Ordre des barreaux“), Liga voor Mensenrechten ASBL („LMR“), Ligue des Droits de l'Homme ASBL („LDH“) a Académie Fiscale ASBL („Académie Fiscale“) podali k předkládajícímu soudu různé ústavní stížnosti proti zmiňovanému zákonu, a tvrdili, souhrnně řečeno, že překročil meze toho, co je nezbytně nutné, a neposkytoval dostatečné záruky ochrany.

18. V tomto kontextu Cour constitutionnelle (Ústavní soud) předkládá Soudnímu dvoru následující otázky:

„1) Musí být čl. 15 odst. 1 směrnice 2002/58/ES ve spojení s právem na bezpečnost zaručeným v článku 6 Listiny základních práv Evropské unie [‚Listina‘] 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/ES, 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 [Evropského parlamentu a Rady] (EU) 2016/679 [ze dne 27. dubna 2016 o ochraně fyzických

[14] – Rozsudek č. 84/2015, *Moniteur belge* ze dne 11. srpna 2015.

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. 2019, L 119, s. 1)], 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/ES ve spojení s články 4, 7 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/ES, 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 8 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 a druhou předběžnou otázku dospět k závěru, že je napadený zákon v rozporu s jednou či více povinnostmi vyplývajícími z ustanovení uvedených v těchto otázkách, mohl by dočasně zachovat účinky [sporného] zákona […], aby mohly být předtím shromážděné a uchované údaje dále využívány pro účely stanovené zákonem?“

III. Řízení před Soudním dvorem

19. Žádost o rozhodnutí o předběžné otázce byla zapsána do rejstříku kanceláře Soudního dvora dne 2. srpna 2018.

20. Písemná vyjádření předložili VZ a další, Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), belgická, česká, dánská, německá, estonská, irská, španělská, francouzská, kyperská, maďarská, nizozemská, polská a švédská vláda a vláda Spojeného království, jakož i Komise.

21. Dne 9. září 2019 se konalo jednání společné s jednáním ve věcech C-511/18, C-512/18 a C-623/17, jehož se zúčastnili účastníci všech čtyř řízení o předběžné otázce, výše uvedené vlády a vláda Norska, jakož i Komise a Evropský inspektor ochrany údajů.

IV. Analýza

22. První předběžná otázka se v podstatě shoduje s otázkami předloženými ve věcech C-511/18 a C-512/28. Odlišuje se nicméně od nich co do cílů, k nimž slouží vnitrostátní právní úprava a jimiž není pouze boj proti terorismu a proti nejzávažnějším formám kriminality nebo zajištění národní bezpečnosti, nýbrž také „obrana území, veřejná bezpečnost, vyšetřování, odhalování a stíhání jiných než závažných trestných činů“ a obecně kterýkoli z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679.

23. Druhá předběžná otázka navazuje na první, ale doplňuje ji o dotaz, zda by pozitivní povinnosti, které v souvislosti s vyšetřováním a trestáním sexuálního zneužívání nezletilých přísluší orgánům veřejné moci, mohly odůvodnit sporná opatření.

24. Třetí otázka je formulována pro případ, že by byl vnitrostátní předpis neslučitelný s unijním právem. Předkládající soud se táže, zda by za tohoto předpokladu bylo možné dočasně zachovat účinky zákona ze dne 29. května 2016.

25. Budu tyto otázky analyzovat v prvé řadě z hlediska použitelnosti směrnice 2002/58 a za tím účelem budu odkazovat na své stanovisko v jiném z těchto řízení o předběžných otázkách. Ve druhé řadě upozorním na základní směry v judikatuře Soudního dvora v této oblasti a možnosti jejich rozvoje. A v poslední řadě nabídnu řešení pro každou jednotlivou z těchto předběžných otázek.

A. Použitelnost směrnice 2002/58

26. Stejně jako v ostatních třech řízeních o předběžné otázce, také v tomto vznikla pochybnost o tom, zda je směrnice 2002/58 použitelná. Vzhledem k totožnosti předběžných otázek předložených členskými státy v tomto ohledu odkazuji na své stanovisko ve věcech C-511/18 a C-512/18 [15].

B. Judikatura Soudního dvora ohledně uchovávání osobních údajů a přístupu k nim veřejnými orgány v rámci směrnice 2002/58

1. Zásada důvěrnosti sdělení a souvisejících údajů

27. Ustanovení směrnice 2002/58 „upřesňují a doplňují“ směrnici 95/46/ES [16] pro účely dosažení vysoké úrovně ochrany osobních údajů v kontextu poskytování služeb elektronických komunikací [17].

28. Článek 5 odst. 1 směrnice 2002/58 uvádí, že členské státy prostřednictvím vnitrostátních právních předpisů zajistí důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů.

29. Důvěrnost sdělení s sebou mimo jiné nese (čl. 5 odst. 1 věta druhá směrnice 2002/58) zákaz uchovávání provozních údajů souvisejících s elektronickou komunikací osobami jinými než uživateli bez souhlasu dotčených uživatelů. Výjimkou jsou „osoby oprávněné zákonem […] a technické uchovávání, které je nezbytné pro přenos sdělení“ [18].

30. Cílem článků 5, 6 a čl. 9 odst. 1 směrnice 2002/58 je zachovat důvěrnosti sdělení a souvisejících údajů a minimalizovat riziko zneužití. Rozsah jejich působnosti musí být posuzován ve spojení s bodem 30 odůvodnění této směrnice, v němž se uvádí, že „systémy pro zajišťování sítí a služeb elektronických komunikací musí být navrženy tak, aby omezily na nutné minimum množství nezbytných osobních údajů“ [19].

15 – Body č. 40 a násl.

16 – 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). Viz čl. 1 odst. 2 směrnice 2002/58. Směrnice 95/46 byla zrušena ode dne 25. května 2018 nařízením 2016/679. Vzhledem k tomu, že směrnice 2002/58 buď odkazuje na směrnici 95/46, nebo nestanoví vlastní pravidla, je nezbytně nutné zohlednit ustanovení tohoto nařízení (viz čl. 94 body 1 a 2 nařízení č. 2016/679).

17 – Rozsudek Tele2 Sverige a Watson, body 82 a 83.

18 – Tamtéž, bod 85 a citovaná judikatura.

19 – Tamtéž, bod 87. Kurzivou zvýraznil autor stanoviska.

31. Těmito údaji mohou být:

– *provozní* údaje, jejichž zpracování a uchovávání je povoleno pouze v rozsahu a na dobu, jež jsou nezbytné pro účely účtování, marketingu těchto služeb a poskytování služeb s přidanou hodnotou (článek 6 směrnice 2002/58). Po uplynutí této doby musí být zpracovávané a uchovávané údaje vymazány nebo anonymizovány [20];

– *lokalizační* údaje odlišné od provozních údajů, které lze zpracovávat pouze tehdy, jsou-li splněny určité podmínky, a poté, co byly anonymizovány, anebo se souhlasem uživatelů nebo účastníků (čl. 9 odst. 1 směrnice 2002/58) [21].

2. Omezující ustanovení obsažená v čl. 15 odst. 1 směrnice 2002/58

32. Článek 15 odst. 1 směrnice 2002/58 umožňuje členským státům „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.

33. Každé omezení musí představovat „v demokratické společnosti nezbytné, přiměřené a úměrné 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 [95/64]“.

34. Povaha takového výčtu je taxativní [22], což příkladmo („mimo jiné“) dokládá možnost přijmout „legislativní opatření umožňující uchovávání údajů po omezenou dobu na základě důvodů uvedených v tomto odstavci“.

35. V každém případě „[v]eškerá 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 založení Evropské unie [Smlouvy o Evropské unii]“. Proto musí být čl. 15 odst. 1 směrnice 2002/58 vykládán ve světle základních práv zaručených Listinou [23].

36. Z těchto práv uznaných v Listině Soudní dvůr zmínil, což je nyní důležité, právo na soukromí (článek 7), právo na ochranu osobních údajů (článek 8) a právo na svobodu projevu (článek 11) [24].

37. Soudní dvůr zároveň jako své výkladové vodítko čl. 15 odst. 1 směrnice 2002/58 vyzdvihl, že omezení povinnosti zajistit důvěrnost sdělení a s ním souvisejících provozních údajů musí být vykládány striktně.

38. Konkrétně odmítl „aby se výjimka z této základní povinnosti, a zejména ze zákazu uchovávání těchto údajů stanoveného v článku 5 této směrnice, stala pravidlem, neboť jinak by bylo posledně uvedené ustanovení zbaveno ve značném rozsahu jeho působnosti“ [25].

[20] – Tamtéž, bod 86 a citovaná judikatura.

[21] – Tamtéž, bod 86 *in fine*.

[22] – Tamtéž, bod 90.

[23] – Tamtéž, bod 91 a citovaná judikatura.

[24] – Tamtéž, bod 93 a citovaná judikatura.

[25] – Tamtéž, bod 89.

39. Toto dvojí zjištění se mi jeví jako rozhodující pro porozumění, proč Soudní dvůr posoudil jako neslučitelné se směrnicí 2002/58 plošné a nerozlišující uchovávání provozních a lokalizačních údajů souvisejících s elektronickou komunikací.

40. Tímto rozhodnutím Soudní dvůr jen „plně“ [26] použil kritérium přiměřenosti, které již uplatnil dříve [27]: „ochrana základního práva na respektování soukromého života na unijní úrovni vyžaduje, aby výjimky z ochrany osobních údajů a její omezení byly činěny v mezích toho, co je naprosto nezbytné“ [28].

3. Přiměřenost uchovávání údajů

a) Nepřiměřenost plošného a nerozlišujícího uchovávání

41. Soudní dvůr uznal, že boj proti závažné trestné činnosti, zejména proti organizované trestné činnosti a terorismu, má zajisté prvořadý význam pro zajištění veřejné bezpečnosti a jeho účinnost může do velké míry záviset na použití moderních vyšetřovacích metod. Dodal, že „[t]akový cíl obecného zájmu, byť se jedná o cíl základní, však nemůže sám o sobě odůvodnit, aby takové opatření spočívající v uchovávání údajů, jaké zavedla směrnice 2006/24, bylo považováno za nezbytné pro účely uvedeného boje“ [29].

42. Pro účely rozpoznání toho, zda se určité opatření tohoto typu omezuje na nezbytně nutné, Soudní dvůr zdůraznil především mimořádnou závažnost jeho zásahu do základních práv zaručených v článcích 7 a 8 Listiny [30]. Mimořádnou závažnost vyplývající právě z toho, že vnitrostátní právní úprava stanovila „plošné a nerozlišující uchovávání *veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztah*[ovalo] *na veškeré prostředky elektronické komunikace*, a uklád[ala] poskytovatelům služeb elektronických komunikací povinnost uchovávat tyto údaje *systematicky a průběžně bez jakékoli výjimky*“ [31].

43. Zásah, který z tohoto opatření plynul pro život občanů, se odráží v tomto posouzení Soudního dvora ohledně dopadů na uchovávání údajů.

Tyto údaje [32]:

– „umožňují dohledání a identifikaci zdroje sdělení a jeho adresáta, zjištění data, času a délky trvání a určení typu sdělení, identifikaci komunikačního vybavení uživatelů a zjištění polohy mobilního komunikačního zařízení“ [33];

– „umožňují zejména zjistit, s kým a jakým způsobem daný účastník nebo registrovaný uživatel komunikoval, stejně jako určit čas této komunikace a místo, ze kterého probíhala. Dále

[26] – Použití tohoto příslovce v rozsudku Tele2 Sverige a Watson, bod 95, vychází z bodu 11 odůvodnění směrnice 2002/58.

[27] – Rozsudek Digital Rights, bod 48: „[s] ohledem na významnou úlohu ochrany osobních údajů z hlediska základního práva na respektování soukromého života, jakož i na rozsah a závažnost zásahu do tohoto práva, jenž směrnice 2006/24 představuje, je posuzovací pravomoc unijního [normotvůrce v projednávané věci omezena, takže přezkum musí být přísný.“

[28] – Rozsudek Tele2 Sverige a Watson, bod 96 a citovaná judikatura.

[29] – Rozsudek Digital Rights, bod 51. V témže smyslu rozsudek Tele2 Sverige a Watson, bod 103.

[30] – Rozsudky Digital Rights, bod 65, a Tele2 Sverige a Watson, bod 100.

[31] – Rozsudek Tele2 Sverige a Watson, bod 97. Kurzivou zvýraznil autor stanoviska.

[32] – Mezi nimi se nacházejí jméno a adresa účastníka nebo registrovaného uživatele, čísla telefonů volajícího i adresáta sdělení a IP adresa pro služby internetu.

[33] – Rozsudek Tele2 Sverige a Watson, bod 98.

umožňují znát četnost komunikace daného účastníka nebo registrovaného uživatele s určitými osobami v určitém období“ [34];

– umožňují „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 jejich aktivitách, společenských vztazích těchto osob a o společenských kruzích, s kterými se stýkají“ [35];

– na jejich základě „lze […] vytvořit profil dotčených osob, který je s ohledem na právo na ochranu soukromého života informací stejně citlivé povahy, jako je samotný obsah sdělení“ [36].

44. Zásah může navíc „v dotčených osobách vyvolávat dojem, že jejich soukromí je pod neustálým dohledem“, neboť „k uchovávání údajů dochází bez vyrozumění uživatelů služeb elektronických komunikací“ [37].

45. Vzhledem k závažnosti zásahu může být takové opatření odůvodněno pouze bojem proti závažné trestné činnosti [38]. Toto opatření se nicméně nemůže změnit v obecné pravidlo, jelikož „režim zavedený směrnicí 2002/58 vyžaduje, aby toto uchovávání údajů bylo výjimkou“ [39].

46. Navíc jsou zde přítomny dva rysy vycházející z toho, že posuzované opatření nestanovilo „žádné rozlišení, omezení nebo výjimky činěné v závislosti na sledovaném cíli“ [40] a „nevyžaduje souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti“ [41]:

– opatření se jednak týká „globálně všech osob, které využívají služeb elektronických komunikací, avšak osoby, jejichž údaje jsou uchovávány, se nenacházejí, byť nepřímo, v situaci, která může vést k trestnímu stíhání […] Kromě toho nestanoví žádnou výjimku, takže se vztahuje i na osoby, jejichž sdělení jsou podle pravidel vnitrostátního práva předmětem profesního tajemství“ [42],

– a jednak „[…] 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“ [43].

47. Za takových podmínek analyzovaná vnitrostátní právní úprava překračuje meze toho, co je naprosto nezbytné. Nelze ji proto 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 [44].

34 – Tamtéž, bod 98.
35 – Tamtéž, bod 99.
36 – Tamtéž, bod 99 *in fine*.
37 – Tamtéž, bod 100.
38 – Tamtéž, bod 102.
39 – Tamtéž, bod 104.
40 – Tamtéž, bod 105.
41 – Tamtéž, bod 106.
42 – Tamtéž, bod 105.
43 – Tamtéž, bod 106.
44 – Tamtéž, bod 107.

b) Proveditelnost cíleného uchovávání údajů

48. Soudní dvůr připustil slučitelnost s unijním právem u takové vnitrostátní úpravy, která „preventivně umožňuje *cílené uchovávání* provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti“ [45].

49. Platnost takového cíleného uchovávání údajů je podmíněna tím, že „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“.

50. Vodítka, která rozsudek Tele2 Sverige a Watson nabízí pro zjištění, kdy jsou tyto podmínky splněny, nejsou (a možná ani nemohou být) vyčerpávající a jsou formulována spíše obecně. Za účelem jejich dodržení členské státy:

– musí zavést jasná a přesná pravidla pro rozsah a použití takového opatření pro uchovávání údajů [46];

– musí stanovit „objektivní[…] kritéri[a a musí existovat] vztah mezi údaji, které mají být uchovávány, a sledovaným účelem“ [47] a

– musí vycházet z „objektivních skutečnost[í], na jejichž základě lze vymezit okruh osob z řad veřejnosti, jejichž údaje mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností nebo určitým způsobem přispívat k boji proti závažné trestné činnosti či k předcházení závažného ohrožení veřejné bezpečnosti“ [48].

51. V souvislosti s těmito objektivními skutečnostmi Soudní dvůr dává jako příklad možnost použít k vymezení veřejnosti a potenciálně dotčených situací zeměpisné kritérium. Poukázání na toto kritérium, o němž se kriticky zmiňovaly některé členské státy, nemá podle mého názoru za cíl omezit výčet přijatelných kritérií cílenosti pouze na něj.

4. Přiměřenost přístupu k údajům

a) Rozsudek Tele2 Sverige a Watson

52. Soudní dvůr se zabývá *přístupem* vnitrostátních orgánů k údajům nezávisle na rozsahu povinnosti *uchovávání* uložené poskytovatelům služeb elektronických komunikací, a zejména na plošné nebo cílené povaze uchovávání těchto údajů [49].

53. V důsledku toho – přestože důvodem pro uchovávání je usnadnit pozdější přístup k údajům – může jedno i druhé způsobit odlišná porušení základních práv chráněných Listinou. Toto rozlišování nicméně neznamená, že by některé úvahy související s uchováváním nebyly také použitelné na přístup k uchovávaným údajům.

45 – Tamtéž, bod 108. Kurzivou zvýraznil autor stanoviska.

46 – Tamtéž, bod 109. Zejména musí vymezit „okolnosti a podmínky, za nichž může být preventivně přijato opatření pro uchovávání údajů, čímž zaručí, že takové opatření se omezí na to, co je nezbytně nutné“.

47 – Tamtéž, bod 110.

48 – Tamtéž, bod 111.

49 – Tamtéž, bod 113.

54. V tomto duchu přístup:

– musí „skutečně a nezbytně odpovídat některému z těchto cílů“ uvedených v čl. 15 odst. 1 větě první směrnice 2002/58. Také musí existovat soulad mezi závažností zásahu a sledovaným cílem. Pokud je zásah kvalifikován jako závažný, může být odůvodněn pouze bojem proti závažné trestné činnosti [50];

– je přípustný pouze v rozsahu, který je nezbytně nutný [51]. Navíc legislativní opatření musí stanovovat „jasná a přesná pravidla, která vymezují okolnosti a podmínky, za nichž mohou poskytovatelé služeb elektronických komunikací poskytnout příslušným vnitrostátním orgánům přístup k údajům. Stejně tak opatření této povahy musí být právně závazná ve vnitrostátním právu“ [52];

– konkrétně vnitrostátní právní úprava musí „hmotněprávní a procesní podmínky, jimiž se řídí přístup příslušných vnitrostátních orgánů k uchovávaným údajům“ [53].

55. Z výše uvedeného lze vyvodit, že „obecný přístup ke všem uchovávaným údajům bez ohledu na jakoukoli přinejmenším nepřímou souvislost se sledovaným cílem nelze považovat za omezený na to, co je nezbytně nutné“ [54].

56. Podle Soudního dvora „musí dotčená vnitrostátní právní úprava vycházet z objektivních kritérií, na jejichž základě jsou vymezeny okolnosti a podmínky, za nichž musí být poskytnut příslušným vnitrostátním orgánům přístup k údajům účastníků nebo registrovaných uživatelů“ [55]. V této souvislosti „lze v zásadě udělit v souvislosti s cílem boje proti trestné činnosti přístup pouze k *údajům osob, u nichž je podezření, že připravují, páchají či spáchaly závažný trestný čin nebo se určitým způsobem na takovém trestném činu podílely*“ [56].

57. Jinými slovy, vnitrostátní právní úprava, na jejímž základě je příslušným vnitrostátním orgánům poskytnut přístup k uchovávaným údajům, musí mít dostatečně omezenou působnost. Musí existovat vztah mezi dotčenými osobami a sledovaným cílem, tak aby přístup nezahrnoval značné množství osob, nebo dokonce všechny osoby, všechny prostředky elektronické komunikace, a všechny uchovávané údaje.

58. Tato pravidla nicméně mohou být za určitých okolností zmírněna. Soudní dvůr zohledňuje „určit[é] situac[e], jako jsou případy, kdy jsou stěžejní zájmy národní bezpečnosti, obrany nebo veřejné bezpečnosti ohroženy teroristickými činnostmi“. V takových situacích „lze rovněž poskytnout přístup k údajům jiných osob, jsou-li dány objektivní skutečnosti, na jejich[ž] základě lze mít za to, že tyto údaje mohou v konkrétním případě účinně přispět k boji proti takovým činnostem“ [57].

[50] – Tamtéž, bod 115.

[51] – Tamtéž, bod 116.

[52] – Tamtéž, bod 117.

[53] – Tamtéž, bod 118.

[54] – Tamtéž, bod 119.

[55] – Tamtéž.

[56] – Tamtéž. Kurzivou zvýraznil autor stanoviska.

[57] – Tamtéž.

59. Toto vyjádření Soudního dvora umožňuje, aby členské státy zavedly zvláštní režim širšího přístupu k údajům, když je to výjimečně nezbytné pro potírání hrozeb prvořadých zájmů státu (národní bezpečnost, obrana a veřejná bezpečnost) [58], způsobem, který zahrnuje dokonce i osoby pouze nepřímo spojené s těmito hrozbami.

60. Přístup vnitrostátních orgánů k uchovávaným údajům, ať už je jejich typ jakýkoli, musí podléhat třem podmínkám:

– musí být „zásadn[ě] […], s výjimkou naléhavých případů, řádně odůvodněn, podléha[t] předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu“. Rozhodnutí tohoto soudního nebo správního orgánu musí být přijato „na základě odůvodněné žádosti těchto příslušných orgánů, zejména v rámci postupů pro předcházení, odhalování nebo stíhání trestných činů“ [59];

– „příslušné vnitrostátní orgány, jimž byl poskytnut přístup k uchovávaným údajům, [musí] o tomto přístupu vyrozumě[t] dotčené osoby v rámci použitelných vnitrostátních postupů, a to od okamžiku, kdy tímto sdělením nebude možné ohrozit probíhající vyšetřování vedené těmito orgány“ [60];

– členské státy musí přijmout předpisy o bezpečnosti a ochraně údajů, které jsou v držení poskytovatelů služeb elektronických komunikací, za účelem zamezení neoprávněnému užití údajů a protiprávnímu přístupu k nim [61].

b) Rozsudek Ministerio Fiscal

61. V této věci vyvstala otázka, zda je vnitrostátní právní předpis, jenž stanoví přístup příslušných orgánů k údajům o občanské totožnosti držitelů některých SIM karet, slučitelný s čl. 15 odst. 1 směrnice 2002/58 vykládaným ve světle článků 7 a 8 Listiny.

62. Soudní dvůr rozhodl, že čl. 15 odst. 1 věta první směrnice 2002/58 neomezuje cíl spočívající v prevenci, vyšetřování, odhalování a stíhání trestných činů výhradně na boj proti závažným trestným činům, ale míří pouze na „trestné činy“ obecně [62].

63. Doplnil, že k odůvodnění přístupu k údajům ze strany příslušných vnitrostátních orgánů musí existovat soulad mezi závažností zásahu a závažností dotčeného trestného činu. V důsledku toho

– „závažný zásah [může být odůvodněn] pouze cílem spočívajícím v boji proti trestné činnosti, která musí být rovněž kvalifikována jako ‚závažná‘ [63]“;

– naproti tomu „v případě, že zásah daný takovým zpřístupněním není závažný, lze jej odůvodnit cílem spočívajícím v prevenci, vyšetřování, odhalování a stíhání ‚trestných činů‘ obecně [64]“.

[58] – Kromě činností teroristů by mohly tuto výjimku odůvodnit další eventuality, jako je kybernetický útok velkého rozsahu na kritickou infrastrukturu státu nebo hrozba spojená s šířením jaderných zbraní.

[59] – Rozsudek Tele2 Sverige a Watson, bod 120.

[60] – Tamtéž, bod 121.

[61] – Tamtéž, bod 122.

[62] – Rozsudek Ministerio Fiscal, bod 53.

[63] – Tamtéž, bod 56.

[64] – Tamtéž, bod 57.

64. Na základě tohoto předpokladu – a na rozdíl od toho, jak postupoval v rozsudku Tele2 Sverige a Watson – Soudní dvůr nekvalifikoval zásah do práv chráněných články 7 a 8 Listiny jako „závažný“, neboť žádost o přístup sloužila „pouze k identifikaci držitelů karet SIM aktivovaných během dvanácti dnů prostřednictvím kódu IMEI odcizeného mobilního telefonu [65]“.

65. Aby zdůraznil menší závažnost zásahu, vysvětlil, že „[ú]daje, kterých se týkala žádost o přístup dotčená ve věci v původním řízení, […] umožňují pro dané období pouze dohledat totožnost držitele SIM karty či SIM karet aktivovaných v odcizeném mobilním telefonu. Bez křížové kontroly údajů o komunikaci vedené z uvedených karet SIM a bez lokalizačních údajů nelze z těchto údajů zjistit datum, čas, délku trvání ani adresáty komunikace uskutečněné prostřednictvím dotčené SIM karty či dotčených SIM karet, ani místo, kde se tato komunikace uskutečnila, či její četnost s určitými osobami v určitém období. Z uvedených údajů tedy nelze vyvodit přesné závěry o soukromí osob, o jejichž údaje se jedná [66]“.

66. Ve věci, ve které byl vynesen rozsudek Ministerio Fiscal, nevyvstala otázka, zda byly osobní údaje, které jsou předmětem přístupu, uchovávány poskytovateli elektronických komunikací v souladu s podmínkami uvedenými v čl. 15 odst. 1 směrnice 2002/58 vykládanými ve světle článků 7 a 8 Listiny [67]. Taktéž se nezkoumala otázka, zda jsou splněny ostatní podmínky přístupu vyplývající z tohoto článku.

67. Z rozsudku Ministerio Fiscal tudíž nelze dovodit žádnou změnu judikatury Soudního dvora o neslučitelnosti vnitrostátního režimu, který povoluje plošné a nerozlišující uchovávání údajů, s unijním právem ve smyslu rozsudku Tele2 Sverige a Watson.

68. Nicméně domnívám se, že Soudní dvůr tím, že uznal platnost režimu omezeného přístupu k určitým osobním údajům (které se týkají občanské totožnosti držitelů SIM karet), implicitně akceptuje uchovávání těchto údajů poskytovateli služeb.

C. Základní výhrady vůči judikatuře Soudního dvora

69. Jak předkládající soud, tak většina členských států, které předložily vyjádření, žádají Soudní dvůr, aby objasnil, upřesnil, nebo dokonce přehodnotil některé aspekty své judikatury v této oblasti, vůči kterým mají výhrady.

70. Větší část těchto výhrad, zastřených nebo přímočarých, již byla vyjádřena v souvislosti s rozsudkem Digital Rights a byla odmítnuta v rozsudku Tele2 Sverige a Watson. Znovu se teď objevují a jejich podstatou je, stručně řečeno, poukázat na to, že by stačily takové přísné normy o přístupu k údajům držených poskytovateli služeb elektronických komunikací, které by mohly určitým způsobem kompenzovat závažnost zásahu, jenž představuje plošné a nerozlišující uchovávání těchto údajů.

[65] – Tamtéž, bod 59. Přístup se týkal „telefonních čísel odpovídajících těmto SIM kartám a údajů o totožnosti držitelů uvedených karet, jako je jejich jméno, příjmení a případně adresa. Tyto údaje se naopak netýkají, jak potvrdila španělská vláda i státní zastupitelství na jednání, komunikace uskutečněné s pomocí odcizeného mobilního telefonu ani jeho lokalizace.“

[66] – Tamtéž, bod 60.

[67] – Rozsudek Ministerio Fiscal, bod 49.

71. V mnoha těchto výtkách se zdůrazňuje také potřeba přijmout skutečně účinná opatření proti závažným hrozbám bezpečnosti a proti trestné činnosti obecně a Soudní dvůr je žádán, aby zohlednil právo na bezpečnost (článek 6 Listiny), jakož i prostor pro uvážení členských států k zachování národní bezpečnosti. V jednom případě se dodává, že Soudní dvůr neuvážil preventivní charakter zásahu bezpečnostních a zpravodajských služeb.

D. Mé posouzení těchto výhrad a upřesnění, která by mohla přinést judikatura Soudního dvora

72. Podle mého názoru by měl Soudní dvůr setrvat na původním názoru, k němuž dospěl v předchozích rozsudcích, a sice že plošná a nerozlišující povinnost uchovávat všechny provozní a lokalizační údaje všech účastníků a registrovaných uživatelů nepřiměřeně porušuje základní práva chráněná články 7, 8 a 11 Listiny.

73. *A contrario* vnitrostátní právní úprava, která by stanovila vhodná omezení pro uchovávání některých z těchto údajů, které byly vytvořeny v kontextu poskytování služeb elektronických komunikací, by mohla být slučitelná s unijním právem. Klíč tedy spočívá v *omezeném uchovávání* těchto údajů.

74. Z důvodů, které dále vysvětlím, by tímto omezením uchovávání neměla být pouze omezení zaměřená na určitou zeměpisnou oblast nebo na určitou kategorii konkrétních osob, protože debaty o těchto kritériích uchovávání odkrývají, že by mohla být nerealizovatelná nebo neúčinná s ohledem na sledované cíle, nebo by se dokonce mohla změnit v zdroj diskriminace.

75. Předesílám, že nesdílím kritický argument, který navrhuje dyádu „širší uchovávání výměnou za omezenější přístup“. Argumentace Soudního dvora, s níž souhlasím, je taková, že uchovávání a přístup k údajům představují dva rozdílné typy zásahu. Přestože uchovávání údajů má smysl s ohledem na možný pozdější přístup ze strany příslušných orgánů, každý z těchto zásahů musí být odůvodněn odděleně, prostřednictvím zvláštního přezkumu ve světle sledovaného cíle.

76. Vnitrostátní systém, který stanoví plošné a nerozlišující uchovávání údajů, nemůže být odůvodněn na základě toho, že příslušné normy nastavují zároveň přísné věcné i procesní požadavky pro přístup k těmto údajům.

77. Musí tedy existovat normy specificky spojené s uchováváním údajů, které pro něj stanoví určité podmínky, aby zabránily jeho plošné a nerozlišující povaze. Jedině tak se zajistí jejich slučitelnost s čl. 15 odst. 1 směrnice 2002/58 ve světle článků 7, 8, 11 a čl. 52 odst. 1 Listiny.

78. To je ostatně přístup zastávaný pracovními skupinami, které vznikly v rámci Rady za účelem definovat pravidla uchovávání a přístupu slučitelná s judikaturou Soudního dvora a které se paralelně zabývají oběma druhy zásahů [68].

79. Při použití omezení na každý z těchto dvou typů zásahů bude možné posoudit, zda jejich případný kumulativní účinek kombinovaný se solidními zárukami zmírní dopad uchovávání údajů na základní práva chráněná články 7, 8 a 11 Listiny a zároveň zajistí účinnost vyšetřování.

[68] – Členské státy jsou od roku 2017 zúčastněny v pracovní skupině, jejímž cílem je přizpůsobit jejich právní předpisy kritériím stanoveným judikaturou Soudního dvora v této oblasti [Groupe Échange d'informations et protection des données (DAPIX)].

80. Systém, aby chránil tato práva, musí:

– stanovit takové uchovávání údajů, které obsahuje určitá omezení a rozlišování v závislosti na sledovaném cíli, a

– upravit přístup k těmto údajům pouze nezbytně nutným způsobem vzhledem ke sledovanému cíli a pod kontrolou soudu nebo nezávislého správního orgánu.

81. Důvodnost, aby poskytovatelé služeb elektronických komunikací uchovávali určité údaje, a to nejen pro plnění svých smluvních povinností vůči uživatelům, sílí paralelně s technologickým pokrokem. Připustí-li se, že je toto uchovávání užitečné pro prevenci a potírání trestné činnosti (která je těžko vymýtitelná[69]), nebylo by podle všeho logické omezovat jeho rozsah na pouhé využívání údajů, které provozovatelé uchovávají, aby mohli provozovat svou obchodní činnost, a to pouze na dobu nezbytnou pro tyto činnosti.

82. Pokud se již uzná užitečnost povinnosti uchovávat údaje pro zachování národní bezpečnosti a pro boj s trestnou činností nad rámec toho, co poskytovatelé mohou činit pro účely svých technických a obchodních potřeb, je nezbytné definovat hranice těchto povinností.

83. Každý režim uchovávání musí striktně odpovídat sledovanému cíli, tak aby se nemohl změnit na nerozlišující uchovávání[70]. Musí zároveň zamezit tomu, aby souhrn těchto údajů poskytl *profil* dotčené osoby (to znamená popis jejích obvyklých činností a jejích sociálních vztahů) blízký nebo podobný tomu, který by bylo možno získat znalostí obsahu sdělení.

84. Za účelem vyjasnění některých nedorozumění a určitých nepochopení je nutno mít na paměti to, co Soudní dvůr *nevyslovil* v rozsudcích Digital Rights a Tele2 Sverige a Watson. V nich nebyla jako taková odmítnuta existence uchovávání údajů coby užitečného nástroje boje proti trestné činnosti. Naopak byla uznána legitimita cíle předcházet trestným činům a potírat je i užitečnost režimu uchovávání údajů za účelem dosažení tohoto cíle.

85. Co tehdy bylo jasně odmítnuto, opakuji, bylo to, aby Unie nebo její členské státy mohly s odvoláním na tento cíl uložit nerozlišující uchovávání *všech* údajů vytvořených při poskytování služeb elektronických komunikací a obecný přístup k těmto údajům.

86. Proto je třeba najít způsoby uchovávání údajů, které nemají charakteristiky („plošné a nerozlišující“) neslučitelné s ochranou vyžadovanou články 7, 8 a 11 Listiny.

87. Jednou z těchto forem by mohlo být *cílené* uchovávání údajů zaměřené buď na specifickou veřejnost (teoreticky na osoby, které vykazují určité více či méně přímé vazby s nejzávažnějšími hrozbami) nebo na určitou zeměpisnou oblast.

88. Tento návrh je nicméně do určité míry problematický, neboť

– identifikace skupiny potenciálních agresorů by byla pravděpodobně nedostatečná, pokud tito používají techniky anonymizace nebo falšují svou totožnost. Výběr těchto skupin by mohl navíc vyústit v režim všeobecného podezření u některých segmentů populace a mohl by být klasifikován jako diskriminační v závislosti na použitém algoritmu, a

[69] – V každém případě určení zpravodajských technik a posouzení jejich účinnosti spadá do prostoru pro uvážení členských států.

[70] – Rozsudek Digital Rights, bod 57, a rozsudek Tele2 Sverige a Watson, bod 105.

– cílení podle zeměpisných kritérií (která k tomu, aby byla účinná, vyžadují zahrnutí nemalých oblastí) vyvolává ty stejné problémy a přidává další, jak uvedl na ústním jednání Evropský inspektor ochrany údajů v souvislosti se stigmatizací určitých oblastí.

89. Navíc by zde mohly existovat určité rozpory mezi preventivním charakterem uchovávání zamířeného na specifickou veřejnost nebo na nějakou zeměpisnou oblast a skutečností, že pachatelé trestných činů nejsou předem známi a není známo ani místo a čas jejich spáchání.

90. V každém případě, nelze vyloučit, že se najdou způsoby cíleného uchovávání založené na těchto kritériích, které by byly užitečné pro dosažení výše uvedených cílů. Přísluší zákonodárné moci každého členského státu nebo celé Unie, aby nastavila tyto modely, které by respektovaly ochranu základních práv chráněných Soudním dvorem.

91. Bylo by chybou se domnívat, že cílené uchovávání údajů přináležejících ke specifické veřejnosti nebo k určité zeměpisné oblasti je jediný způsob, který Soudní dvůr shledává slučitelným s čl. 15 odst. 1 směrnice 2002/58, vykládaným ve světle článků 7 a 8 Listiny.

92. Trvám na tom, že lze nalézt jiné způsoby cíleného uchovávání údajů, než jsou formy zaměřené na zvláštní skupiny osob nebo zeměpisné oblasti. Ve skutečnosti jsou téhož mínění pracovní skupiny Rady, o nichž jsem se výše zmiňoval a které jakožto o způsobech řešení uvažovaly konkrétně o omezení kategorií uchovávaných údajů[71], pseudonymizaci údajů[72], zavedení omezené doby uchovávání[73], vyloučení určitých kategorií poskytovatelů služeb elektronických komunikací[74], obnovitelnost schvalování uchovávání[75], povinnost uchovávat shromážděné údaje uvnitř Unie nebo systematická a průběžná kontrola – nezávislým správním orgánem – záruk nabízených poskytovateli služeb elektronických komunikací proti neoprávněnému užívání údajů.

93. Podle mého názoru by se v zájmu souladu s judikaturou Soudního dvora mělo upřednostnit dočasné uchovávání některých *kategorií* provozních a lokalizačních údajů, omezených v závislosti na nezbytných potřebách bezpečnosti, které by neumožňovaly v souhrnu získat přesný a detailní obraz o životě dotčených osob.

94. V praxi to znamená, že co se týče dvou základních kategorií (provozních a lokalizačních údajů), mohou být prostřednictvím vhodných filtrů uchovávány *minimální* údaje, které se považují za absolutně nezbytné pro předcházení a účinnou kontrolu trestné činnosti a ochranu národní bezpečnosti.

[71] – Údaje, které nejsou nezbytně nutné a objektivně potřebné pro předcházení trestným činům a jejich stíhání a pro ochranu veřejné bezpečnosti, by byly vyňaty z povinnosti uchovávání. Zejména by bylo potřebné – v souladu se sledovaným cílem – uvést, které typy údajů o účastnících, provozních a lokalizačních údajů by měly být povinně uchovávány za účelem dosažení tohoto cíle. Zejména by byly vyloučeny údaje, které nejsou považovány za nezbytné pro vyšetřování a stíhání trestných činů.

[72] – Metoda, pomocí níž se jména nahradí přezdívkou a údaje tak již nejsou svázány se jménem. Na rozdíl od anonymizace umožňuje pseudonymizace zpětně spojit údaje se jménem dotyčné osoby.

[73] – Bylo by možné zabývat se možností upravit dobu uchovávání v závislosti na různých kategoriích údajů s ohledem na jejich povahu více či méně narušující soukromý život osob. Navíc by bylo nutné stanovit, že údaje budou po skončení doby uchovávání trvale odstraněny.

[74] – Bylo by možné uvažovat o možnosti neukládat povinnost uchovávat údaje všem poskytovatelům služeb elektronických komunikací, nýbrž uložit tuto povinnost podle jejich velikosti a typu služeb, které nabízejí, a vyjmout například ty, kteří poskytují vysoce specializované služby.

[75] – Systémy povolování by se mohly zakládat na periodickém hodnocení hrozeb v každém členském státě. Musí být zajištěno, že vztah mezi uchovávanými údaji a sledovaným cílem by se tvořil a přizpůsoboval specifické situaci v každém členském státě. Proto by bylo možné, aby povolení k uchovávání udělená poskytovatelům mohla vést k uchovávání určitých typů údajů v určitém časovém období v závislosti na hodnocení hrozby. Taková povolení by mohla být udělována soudem nebo nezávislým správním orgánem a vyžadovala by periodický přezkum nezbytnosti tohoto uchovávání.

95. Přísluší členským státům nebo unijním institucím, aby legislativní cestou (s pomocí svých vlastních odborníků) realizovaly takové cílení a odolaly jakémukoli nutkání uložit povinnost plošného a nerozlišujícího uchovávání všech provozních a lokalizačních údajů.

96. Kromě tohoto omezení podle kategorií mohou být shromážděné údaje uchovávány pouze po dobu uchovávání tak, aby neumožnily poskytnout podrobný obraz o životě dotčených osob. Tato doba uchovávání navíc musí být uzpůsobena povaze těchto údajů tak, aby údaje poskytující přesnější informace o stylu života a zvycích osob byly uchovávány po kratší dobu [76].

97. Jinými slovy, rozlišování doby uchovávání jednotlivých kategorií údajů v závislosti na jejich užitečnosti pro dosažení cílů bezpečnosti je jednou z cest, která by měla být zvažována. Omezením doby, po kterou se jednotlivé kategorie údajů uchovávají současně (a proto mohou být použity k nalezení souvislostí, které odkrývají životní styl dotčených osob), rozšiřuje ochranu práva zaručeného článkem 8 Listiny.

98. V tomto smyslu se vyjádřil Evropský inspektor ochrany údajů na jednání, totiž že čím více kategorií je v uchovávaných metadatech a čím delší je doba uchovávání, tím snazší je určit detailní profil určité osoby, a naopak [77].

99. Kromě toho, jak se rovněž ukázalo na jednání, je těžké vymezit hranice mezi určitými metadaty elektronických sdělení a obsahem těchto sdělení. Některá metadata mohou být stejně tak odhalující nebo ještě více než samotný obsah těchto komunikací, jak tomu může být v případě adres (URL) navštěvovaných internetových stránek [78]. Tomuto druhu údajů a jemu podobným je proto třeba věnovat zvláštní pozornost, aby byla maximálně omezena potřeba jejich uchovávání a doba, po kterou jsou uchovávány.

100. Nalézt vyvážené řešení není jednoduché, neboť technika propojování uchovávaných údajů a jejich uvádění do souvislostí umožňuje orgánům činným v trestním řízení zjistit totožnost podezřelého, resp. zpravodajským službám identifikovat hrozbu. I když je tomu tak, je velký rozdíl mezi uchováváním údajů za účelem odhalení tohoto podezřelého nebo této hrozby a takovým uchováváním, jehož výsledkem je nabídka detailního obrazu života určité osoby.

101. Nemyslím si, že než bude přijata právní regulace společná pro celou Unii v této specifické oblasti, je možné žádat od Soudního dvora, aby převzal regulatorní funkce a detailně upřesňoval, které kategorie údajů mohou být uchovávány a po jak dlouhou dobu. Přísluší unijním orgánům a členským státům, aby po nastavení mantinelů, které podle Soudního dvora vyplývají z Listiny, určily ten správný bod, ve kterém dojde k dosažení rovnováhy mezi ochranou bezpečnosti a základními právy chráněnými Listinou.

102. Je jasné, že vzdát se informací dovoditelných z velkého množství uchovávaných údajů by mohlo v některých případech ztížit boj proti potenciálním hrozbám. To je však jedna z daní, kterou veřejná moc musí zaplatit, když sama sobě ukládá povinnost chránit základní práva.

[76] – To je podle všeho systém uplatňovaný ve Spolkové republice Německo, jejíž vláda na ústním jednání uvedla, že podle jejích předpisů je doba uchovávání provozních údajů deset týdnů, zatímco doba uchovávání lokalizačních údajů jsou jen čtyři týdny. Naproti tomu podle Francouzské republiky je nezbytné uchovávat provozní a lokalizační údaje po dobu jednoho roku. Podle tohoto členského státu by zkrácení doby na méně než rok mělo za důsledek snížení účinnosti služeb soudní policie.

[77] – Samozřejmě je nutno zaručit, aby poskytovatelé služeb elektronických komunikací údaje trvale odstranili po skončení doby uchovávání (s výjimkou těch, které mohou nadále uchovávat pro obchodní účely v souladu se směrnicí 2002/58).

[78] – Na jednání francouzská vláda uvedla, že adresy URL byly vyloučeny z údajů o připojení, pro něž právní předpisy stanovily obecnou povinnost uchovávání.

103. Stejně jako by nikdo nepodporoval povinnost *ex ante* plošného a nerozlišujícího uchovávání *obsahu* soukromých elektronických sdělení (a to ani tehdy, kdyby zákon zaručoval pozdější omezený přístup k těmto obsahům), nemohou být ani metadata těchto sdělení, která mohou obsahovat stejně citlivé informace, jako je samotný obsah, předmětem nerozlišujícího a plošného uchovávání.

104. Legislativní obtížnost – kterou uznávám – nastavit přesně případy a podmínky, za nichž je třeba provádět cílené uchovávání, neospravedlňuje to, aby členské státy z výjimky učinily pravidlo a z plošného uchovávání osobních údajů učinily centrální zásadu svých právních úprav. Pokud by tomu tak bylo, připustilo by se na dobu neurčitou zásadní oslabení práva na ochranu osobních údajů.

105. Musím dodat, že nic 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 v tak širokém rozsahu, jak by bylo nezbytně nutné.

106. Za těchto okolností by mohla být přijata právní úprava, která by konkrétně umožňovala uchovávání údajů (a přístup k nim) šířeji, podle podmínek a postupů, které by těmto opatřením zajistily mimořádnost co do věcného rozsahu a doby jejich trvání i příslušné soudní záruky.

107. Komparativní studie právních režimů upravujících ústavně krizové situace ukazují, že není nemožné vymezit skutkové případy, které by byly způsobilé vyvolat uplatnění zvláštního normativního režimu, a určit, který orgán může přijmout toto rozhodnutí, za jakých podmínek a pod čím dohledem [79].

E. Konkrétní odpovědi na tři předběžné otázky

1. Úvodní poznámka

108. Předkládající soud žádá o výklad čl. 15 odst. 1 směrnice 2002/58 v souvislosti s různými právy zaručenými Listinou, a sice s právem na respektování soukromého a rodinného života (článek 7), právem na ochranu osobních údajů (článek 8) a právem na svobodu projevu a informací (článek 11).

109. Jak vysvětluji ve stanovisku ve věcech C-511/18 a C-512/18, jde totiž o práva, která podle Soudního dvora mohou být v takových případech dotčena.

110. Nicméně Cour constitutionnelle (Ústavní soud) předkládá k posouzení také článek 4 Listiny, jehož se týká druhá předběžná otázka, a článek 6 Listiny, dotčený v první předběžné otázce.

111. Článku 6 Listiny, který zaručuje právo na svobodu a bezpečnost, se týkají i věci C-511/18 a C-512/18 a ohledně jeho případnosti jsem se vyslovil v příslušném stanovisku, na které tímto odkazuji [80].

[79] – Ackerman, B., „The Emergency Constitution“, *Yale Law Journal*, č. 113, 2004, s. 1029 až 1092; Ferejohn, J., a Pasquino, P., „The Law of the Exception: A typology of Emergency Powers“, *International Journal of Constitutional Law*, č. 2, 2004, s. 210 až 239.

[80] – Stanovisko ve věcech C-511/18 a C-512/18, body 95 a násl.

112. Co se týče článku 4 Listiny, považuji vzhledem k tomu, že odpověď nezávisí ani tolik na analýze vnitrostátních předpisů a jejich srovnání s unijním právem, jako spíše na výkladu tohoto ustanovení, za vhodné podat odpověď nejprve na něj.

2. Ke druhé předběžné otázce

113. Zákazu mučení a nelidského či ponižujícího zacházení anebo trestu zaručený článkem 4 Listiny se totiž týká jen toto řízení o předběžné otázce, a proto je třeba mu věnovat pozornost.

114. Odkazem na článek 4 Listiny chce předkládající soud dát najevo, že vnitrostátní norma má za cíl splnit také *pozitivní povinnost*, která spočívá na veřejné moci, a to povinnost stanovit „právn[í] rám[ec], 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[81]“.

115. Podle mého názoru tato konkrétní *pozitivní povinnost* není příliš odlišná od všech jednotlivých zvláštních povinností, do nichž se z hlediska státu promítá vyhlášení katalogu základních práv. Právo na život (článek 2 Listiny), právo na nedotknutelnost lidské osobnosti (článek 3 Listiny) nebo na ochranu osobních údajů (článek 8 Listiny), stejně jako svoboda projevu (článek 11 Listiny) nebo myšlení, svědomí a náboženského vyznání (článek 10 Listiny) znamenají pro stát povinnost nastavit právní rámec, v němž bude jejich skutečné využívání zaručeno, případně prostřednictvím výkonu monopolizované síly veřejné moci, proti komukoli, kdo by mu bránil nebo jej ztěžoval[82].

116. Co se týče sexuálního zneužívání nezletilých, ESLP rozhodl, že děti a další zranitelné osoby mají kvalifikované právo na ochranu ze strany státu prostřednictvím přijetí trestněprávních norem, které účinným způsobem trestají tyto trestné činy a mají odrazující účinky[83].

117. Toto kvalifikované právo nachází oporu nejen v článku 4 Listiny, neboť přirozeně se lze dovolat článku 1 (lidská důstojnost) nebo článku 3 (právo na fyzickou a psychickou nedotknutelnost).

[81] – Formulace druhé otázky *in fine*. Tento odkaz na elektronické komunikační prostředky vysvětluje, že otázka zmiňuje druhou *pozitivní povinnost*, která leží na státech a je uložena článkem 8 Listiny ohledně ochrany osobních údajů. Z dvojího odkazu na článek 8 Listiny vyplývá, že předkládající soud připisuje právům zakotveným v Listině v závislosti na jejich povaze dvojí účel, a sice jako *mez* sporné povinnosti a jako *odůvodnění* této povinnosti.

[82] – Tato povinnost účinnosti se v sociálním nebo pečovatelském státě, v němž je kromě formálního uznání práv důležitá praktická realizace jejich materiálního obsahu, projevuje povinností veřejné moci dosáhnout výsledku.

[83] – Rozsudek ESLP ze dne 2. prosince 2008, K. U. proti Finsku, (ECHR:2008:1202JUD000287202), bod 46.

118. Přestože pozitivní povinnost veřejné moci zajistit ochranu dětí a dalších zranitelných osob nelze ponechat stranou při vážení právních zájmů dotčených vnitrostátními předpisy [84], také se nemůže změnit v „nepřiměřenou zátěž“ pro veřejnou moc [85] ani ji nelze splnit za hranicí legality nebo respektování ostatních základních práv [86].

3. K první předběžné otázce

119. Podstatou otázky předkládajícího soudu je, zda unijní právo brání vnitrostátnímu právnímu předpisu, o jehož protiústavnosti má rozhodnout v příslušném řízení.

120. Vzhledem k tomu, že Soudní dvůr již podal výklad směrnice 2002/58, který je v souladu s příslušnými ustanoveními Listiny, musí odpověď na předběžnou otázku zohledňovat judikaturu vycházející z rozsudku Tele2 Sverige a Watson, v tomto případě s drobnými odlišnostmi, které nyní doplním.

121. Vycházeje z tohoto předpokladu, musí být výkladová vodítka, která je možné poskytnout Cour constitutionnelle (Ústavní soud) k tomu, aby sám posoudil slučitelnost vnitrostátního předpisu s unijním právem, dána odděleně pro uchovávání údajů a pro přístup k nim, tak jak je to upraveno v této vnitrostátní normě.

a) K podmínkám pro uchovávání údajů

122. Belgická vláda zdůrazňuje, že si přála vytvořit jasný právní rámec, který by zahrnoval potřebné záruky ochrany soukromého života, a nikoli vycházet z praxe poskytovatelů služeb elektronických komunikací týkající se uchovávání údajů za účelem účtování a vyřizování žádostí o informace ze strany zákazníků.

123. Podle této vlády obecná a preventivní povinnost uchovávání údajů nemá za cíl pouze vyšetřování, odhalování a stíhání závažných trestných činů, nýbrž také zachování národní bezpečnosti, ochranu území a veřejnou bezpečnost, vyšetřování, odhalování a stíhání jiných než závažných trestných činů, nebo předcházení zakázaného použití systémů elektronických komunikačních systémů [87], anebo kterýkoli jiný z důvodů uvedených v čl. 23 odst. 1 nařízení 2016/679.

124. Podle belgické vlády:

– uchovávání údajů jako takové neumožňuje dovodit velmi přesné závěry o soukromém životě dotčených osob, protože možnost dovodit takové závěry by přineslo pouze opatření, které by umožnilo také přístup k uchovávaným údajům;

[84] – V tomto ohledu se domnívám, že k právům, která zmiňuje předkládající soud (jakožto *meze* sporné povinnosti, nikoli její *odůvodnění*), by bylo možné doplnit právo na účinnou právní ochranu (článek 47 Listiny) nebo právo na obhajobu (článek 48 Listiny), o jehož případném porušení se v původních řízeních také vedla debata. Nicméně výroková část předkládacího usnesení se zmiňuje pouze o článcích 7, 8, 11 a čl. 52 odst. 1 Listiny.

[85] – Rozsudek ESLP ze dne 28. října 1998, Osman proti Spojenému království (CE:ECHR:1998:1028JUD002345294), bod 116.

[86] – Tamtéž, bod 116 *in fine*: „[je nezbytné] zajistit, aby policie vykonávala pravomoc potlačování a prevence trestné činnosti za plného respektování zákonných prostředků a dalších záruk, které legitimně omezují dopad jejích úkonů v rámci trestního stíhání“. Stejně tak viz rozsudek ESLP ze dne 2. prosince 2008, K. U. proti Finsku (CE:ECHR:2008:1202JUD000287202), bod 48. V témže duchu Soudní dvůr v rozsudku ze dne 29. července 2019, Gambino a Hyka (C-38/18, EU:C:2019:628), bod 49, rozhodl, že práva stanovená ve prospěch oběti trestného činu nemohou mít dopad na účinný výkon procesních práv přiznaných obviněnému.

[87] – Také je odůvodněná pro možnost odpovědi na volání tísňové linky nebo za účelem nalezení pohřešované osoby, jejíž fyzická integrita je v bezprostředním nebezpečí.

– zákon obsahuje kautely určené k ochraně soukromí; kromě jiného se uchovávání nedotýká obsahu sdělení, jsou zde záruky týkající se odůvodnění uchovávání, právo na přístup, právo na opravu a další jsou plně použitelná, poskytovatelé a provozovatelé musí ve vztahu k uchovávaným údajům dodržet stejné povinnosti a opatření k zabezpečení a ochraně, která platí pro údaje v síti, a musí zabránit jejich náhodnému nebo protiprávnímu zničení nebo jejich náhodné ztrátě nebo změně;

– údaje mohou být uchovávány po dobu dvanácti měsíců (po jejichž uplynutí musí být zlikvidovány) a pouze na území Unie;

– poskytovatelé a provozovatelé musí uplatnit opatření k ochraně technologií, které zajišťují, že uchovávané údaje jsou ihned po uložení nečitelné a nepoužitelné pro jakoukoli neoprávněnou osobu, která by k nim získala přístup;

– v každém případě se tyto operace provádějí pod dohledem belgického regulátora poštovních a telekomunikačních služeb a Úřadu pro ochranu osobních údajů.

125. Navzdory těmto zárukám je jisté, že belgické právní předpisy ukládají provozovatelům a poskytovatelům služeb elektronických komunikací plošnou a nerozlišující povinnost uchovávat provozní a lokalizační údaje ve smyslu směrnice 2002/58 zpracovávané v souvislosti s poskytováním těchto služeb. Doba uchovávání je, jak již bylo řečeno, obecně dvanáct měsíců, přičemž není zakotveno žádné časové omezení v závislosti na kategoriích uchovávaných údajů.

126. Tato povinnost obecného a nerozlišujícího uchovávání platí stále a trvale. Přestože jejím důvodem je předcházení, vyšetřování a stíhání všech druhů trestných činů (od těch, které mají vazbu na národní bezpečnost, obranu nebo obzvláště závažných, až k těm, za které lze uložit trest odnětí svobody kratší než jeden rok), povinnost této povahy není v souladu s judikaturou Soudního dvora, takže nemůže být shledána slučitelnou s Listinou.

127. Belgický zákonodárce bude muset k dosažení souladu s touto judikaturou hledat jiné způsoby (jak jsem již výše zmínil), které zavedou pravidla omezeného uchovávání. Tato pravidla, která mohou být v závislosti na kategorii údajů různá, musí ve shodě se zásadou, že lze uchovávat pouze nezbytně nutné *minimum* údajů v závislosti na riziku či hrozbě a po omezenou dobu, která bude záviset na povaze uchovávaných informací. V každém případě z uchovávání nesmí být možné přesně *zmapovat* osobní život, zvyky, chování nebo sociální vztahy dotčených osob.

b) K podmínkám pro přístup veřejných orgánů k uchovávaným údajům

128. Podle mého názoru jsou podmínky uvedené v rozsudku Tele2 Sverige a Watson [88] relevantní také pro přístup, neboť vnitrostátní právní úprava musí stanovit hmotněprávní a procesní podmínky, jimiž se řídí přístup příslušných orgánů k uchovávaným údajům [89].

129. Belgická vláda upřesňuje, že čl. 126 odst. 2 zákona z roku 2005 (o elektronických komunikacích) [90] restriktivně stanoví, které vnitrostátní orgány mohou získat údaje uchovávané podle odstavce 1 téhož článku.

[88] – Viz bod 60 tohoto stanoviska.

[89] – Rozsudek Tele2 Sverige a Watson, bod 118.

[90] – Článek 126 ve znění zákona ze dne 29. května 2016.

130. Mezi těmito orgány se nacházejí soudy jako takové a státní zastupitelství; bezpečnostní složky státu; Bezpečnostní a informační služba, pod kontrolou příslušných nezávislých komisí; příslušníci soudní policie z Belgického institutu poštovních a telekomunikačních služeb; záchranné složky; příslušníci soudní policie z Jednotky pro pohřešované osoby Federální policie; Mediační služba pro telekomunikace a orgány dohledu v odvětví finančnictví.

131. V obecné rovině belgická vláda tvrdí, že vnitrostátní předpisy neumožňují, aby různé služby měly přístup k údajům za účelem aktivního sledování neidentifikovaných hrozeb nebo bez konkrétních indicií. Vnitrostátní orgány tedy nemohou jen tak přistupovat k primárním komunikačním údajům a automatizovaně je zpracovávat za účelem získávání informací a aktivnímu předcházení bezpečnostních hrozeb.

132. Podle téže vlády podléhá přístup k údajům přísným podmínkám v závislosti na postavení každého z příslušných vnitrostátních orgánů.

133. Odpověď na první předběžnou otázku podle mého názoru nevyžaduje, aby Soudní dvůr prováděl vyčerpávající analýzu podmínek, které platí pro možnost těchto jednotlivých orgánů získat uchovávané údaje. Tento úkol přísluší spíše předkládajícímu soudu, který jej musí splnit s ohledem na vodítka vyplývající z judikatury Tele2 Sverige a Watson a Ministerio Fiscal.

134. Dále podle informací předložených belgickou vládou jsou značné rozdíly mezi podmínkami přístupu, které se týkají soudů nebo státního zastupitelství[91] s cílem vyšetřování, odhalování a stíhání trestných činů podle článků 46 *bis*[92] a 88 *bis*[93] trestního řádu, a těmi, které platí pro ostatní orgány.

135. Co se týče bezpečnostních a zpravodajských služeb, podle zákona z roku 1998 musí být žádost o přístup k provozním a lokalizačním údajům, které jsou v držení provozovatelů, podložena objektivními kritérii k zajištění její omezenosti na to, co je nezbytně nutné na základě předem identifikované hrozby[94]. Stanoví se různé doby přístupu (šest, devět nebo dvanáct měsíců) v závislosti na potenciální hrozbě a žádost musí být v souladu se zásadami proporcionality a subsidiarity. Byly zároveň nastaveny mechanismy kontroly vykonávané nezávislým orgánem[95].

[91] – O vhodnosti toho, aby státní zastupitelství přijímalo opatření tohoto typu, se diskutuje v řízení o předběžné otázce ve věci C-746/18, HK v. Prokuratur, které ještě probíhá.

[92] – Pro žádosti o identifikační údaje od provozovatelů je příslušné státní zastupitelství, které tak činí prostřednictvím odůvodněného rozhodnutí a písemně (ústně v naléhavých případech), v němž je odůvodněna přiměřenost opatření ve vztahu k respektování soukromého života a jeho subsidiarita ve vztahu k jakékoli jiné vyšetřovací povinnosti. U trestných činů, za něž nelze uložit trest odnětí svobody v délce jednoho roku nebo vyšší trest, může státní zastupitelství žádat o údaje za období šesti měsíců předcházejících rozhodnutí.

[93] – Pro žádost o sledování elektronických komunikací nebo získání uchovávaných provozních a lokalizačních údajů od provozovatelů je příslušný vyšetřující soudce, který může přijmout toto opatření, pokud existuje důvodné podezření o spáchání trestného činu, za nějž lze uložit určitý trest, a činí tak prostřednictvím odůvodněného a písemného usnesení (ústně v naléhavých případech), které podléhá týmž požadavkům proporcionality a subsidiarity, které platí pro státní zastupitelství. Existuje několik výjimek, pokud se toto opatření vztahuje na určité kategorie chráněných profesí (například na advokáty nebo lékaře).

[94] – V rozhodnutí se v závislosti na konkrétním případu uvedou fyzické nebo právnické osoby, sdružení nebo skupiny, předměty, místa, události nebo informace, na které se vztahuje zvláštní metoda. Také musí být uvedena spojitosti mezi účelem požadovaných údajů a možnou hrozbou, která odůvodňuje tuto zvláštní metodu.

[95] – Správní komise pro dohled nad zvláštními a výjimečnými metodami sběru dat ze strany zpravodajských a bezpečnostních služeb (Komise BIM) a Výbor pro stálou kontrolu zpravodajských služeb (Výbor R). Belgická vláda uvádí, že Komise BIM je odpovědná za dohled nad metodami vyhledávání používanými zpravodajskými a bezpečnostními službami, nad nimiž vykonává kontrolu v první linii. Tato komise, složená ze soudců, plní své úkoly zcela nezávisle. Také se provádějí nezávislé kontroly ve druhé linii, a to v režii Výboru R.

136. Co se týče příslušníků soudní policie z Belgického institutu poštovních a telekomunikačních služeb (BIPT), jejich přístup je možný pod dohledem státního zastupitelství ve velmi omezených konkrétních případech [96], přičemž jejich činnost podle belgické vlády nedosahuje na osoby, jejichž údaje se uchovávají.

137. Záchranné služby, které poskytují pomoc na místě, mohou žádat údaje volajícího, neobdrží-li v návaznosti na tísňové volání od poskytovatele nebo provozovatele identifikační údaje volajícího nebo obdrží-li neúplné nebo nesprávné údaje.

138. Co se týče příslušníků soudní policie přidělených k Jednotce pro pohřešované osoby Federální policie, tito mohou požádat provozovatele o údaje potřebné pro nalezení pohřešovaného, jehož fyzická integrita je bezprostředně ohrožena. Přístup podléhající přísným podmínkám je omezen na údaje k identifikaci uživatele a údaje o přístupu a připojení koncového zařízení k síti nebo službě a o umístění tohoto zařízení a časově na údaje uchovávané po dobu 48 hodin před podáním žádosti.

139. Co se týče Mediační služby pro telekomunikace, tato může požadovat pouze identifikační údaje osoby, která neoprávněně použila síť nebo službu elektronických komunikací. V tomto případě neexistuje předchozí kontrola ze strany soudu nebo nezávislého správního orgánu (odlišného od samotné služby).

140. A konečně s cílem bojovat proti finanční kriminalitě může orgán dohledu v odvětví finančnictví získat přístup k provozním a lokalizačním údajům, který podléhá předchozímu schválení vyšetřujícího soudce.

141. Z uvedení těchto způsobů a podmínek přístupu k uchovávaným údajům platných pro jednotlivé orgány oprávněné k jejich získání vyplývá rozmanitost předpokladů a záruk, jejichž podrobné posouzení vzhledem ke kritériím uplatňovaným Soudním dvorem v jeho judikatuře [97] přísluší předkládajícímu soudu.

142. Poznamenávám například, že v kontextu sporné právní úpravy příslušné vnitrostátní orgány podle všeho nemají povinnost systematicky informovat dotčené osoby (s výjimkou případu, kdy by taková informace zmařila probíhající vyšetřování) o tom, že proběhl přístup k jejich údajům. Také nic nenasvědčuje tomu, že by byla nastavena, přinejmenším pro některé případy, jako jsou finanční trestné činy a přestupky, předem definovaná pravidla týkající se závažnosti těchto protiprávních jednání odůvodňující přístup k příslušným údajům. Vztah mezi intenzitou zásahu a závažností vyšetřovaného trestného činu ve smyslu rozsudku Ministerio Fiscal není ve všech případech zjevný.

143. V každém případě se domnívám, že úvahy týkající se přístupu orgánů k údajům se dostávají do pozadí, když je, jak jsem již vysvětlil, samotné plošné a nerozlišující uchovávání těchto údajů hlavním důvodem, proč je vnitrostátní právní úprava, jíž se týká tato předběžná otázka, v rozporu s unijním právem.

[96] – Pro účely vyšetřování, odhalování a stíhání porušení článků 114 (bezpečnost sítí), 124 (důvěrnost elektronických komunikací) a 126 (uchovávání dat a přístupu k nim) zákona ze dne 13. června 2005 o elektronických komunikacích.

[97] – Odkazuji na bod 60 tohoto stanoviska.

4. K třetí předběžné otázce

144. Cour constitutionnelle (Ústavní soud) se táže, zda za předpokladu, že ve světle odpovědi Soudního dvora bude vnitrostátní právní úprava prohlášena za neslučitelnou s unijním právem, by mohly být dočasně zachovány účinky této právní úpravy. Zabránilo by se tak právní nejistotě a umožnilo by se, aby shromážděné a uchovávané údaje mohly být dále používány ke sledovaným cílům.

145. Z ustálené judikatury vyplývá, že „pouze Soudní dvůr může výjimečně a z naléhavých důvodů právní jistoty přechodně pozastavit vylučovací účinek, který vyvolává pravidlo unijního práva ve vztahu k vnitrostátnímu právu, které je s ním v rozporu“. Pokud by „byly vnitrostátní soudy oprávněny přiznat vnitrostátním ustanovením přednost před unijním právem, byť dočasnou, bylo by tím dotčeno jednotné použití unijního práva [98]“.

146. Komise je toho názoru, že když Soudní dvůr časově neomezil účinky výkladu čl. 15 odst. 1 směrnice 2002/58, odpověď na tuto otázku předkládajícího soudu by měla být záporná [99].

147. Soudní dvůr nicméně v rozsudku ze dne 28. února 2012, Inter-Environnement Wallonie a Terre wallonne [100], uvedl, že s ohledem na existenci naléhavého zájmu týkajícího se ochrany životního prostředí může být vnitrostátnímu soudu výjimečně umožněno využít vnitrostátního ustanovení, které ho opravňuje zachovat určité účinky vnitrostátního aktu, který zrušil pro rozpor s unijní normou [101].

148. Tato judikatorní linie byla potvrzena rozsudkem ze dne 29. července 2019, Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen [102]. I když byla přijata v oblasti ochrany životního prostředí, resp. vycházela z bezpečnosti dodávek elektřiny, nenacházím důvody, proč by mělo být odmítnuto její použití v jiných oblastech unijního práva, zejména v oblasti dotčené v projednávané věci.

149. Pokud nějaký „naléhavý zájem týkající se ochrany životního prostředí“ může odůvodnit, aby vnitrostátní soudy výjimečně zachovaly některé účinky vnitrostátního ustanovení neslučitelného s unijním právem, je to proto, že ochrana životního prostředí je „jedním ze základních cílů Unie a má průřezovou i základní povahu [103]“.

150. Mezi cíle Unie se počítá také vytvoření prostoru bezpečnosti (článek 3 SEU), který zahrnuje respekt k základním funkcím státu, obzvláště k těm, jejichž předmětem je zajištění veřejného pořádku a ochrana národní bezpečnosti (čl. 4 odst. 2 SEU). To je cíl o nic méně „průřezový a zásadní“ než ochrana životního prostředí, jelikož jeho realizace je nezbytnou podmínkou k tomu, aby byl nastaven právní rámec způsobilý zaručit skutečné využívání základních práv a svobod.

98 – Rozsudek ze dne 28. července 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603), bod 33.

99 – Bod 100 písemného vyjádření Komise.

100 – Věc C-41/11, EU:C:2012:103.

101 – Rozsudek ze dne 28. února 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11, EU:C:2012:103), bod 58. V rozsudku ze dne 28. července 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603), bod 34, Soudní dvůr z toho dovodil vůli „přizn[at] vnitrostátnímu soudu výjimečně a v jednotlivém případě možnost zmírnit účinky zrušení vnitrostátního ustanovení, o němž bylo rozhodnuto, že je neslučitelné s unijním právem“.

102 – Věc C-411/17 (EU:C:2019:622), bod 178.

103 – Rozsudek ze dne 28. února 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11, EU:C:2012:103), bod 57.

151. Podle mého názoru by naléhavé zájmy týkající se ochrany národní bezpečnosti mohly v této věci odůvodnit, aby Soudní dvůr předkládajícímu soudu výjimečně umožnil zachovat přinejmenším některé účinky sporného zákona.

152. Toto zachování by vyžadovalo, aby předkládající soud s ohledem na rozhodnutí Soudního dvora uznal vnitrostátní ustanovení za neslučitelné s unijním právem a dopady, které by jeho okamžité zrušení (pokud by zrušení ve vnitrostátním právu bylo důsledkem této neslučitelnosti) nebo zdržení se jeho uplatňování mohlo mít na veřejnou bezpečnost či na bezpečnost státu, za mimořádně narušující.

153. Dočasné zachování (všech nebo některých) účinků vnitrostátního ustanovení by navíc vyžadovalo, aby:

– účelem tohoto prodloužení bylo vyhnout se právnímu vakuu, které by mělo tak škodlivé dopady jako použití sporné právní úpravy, kterému by bylo nemožné čelit jinými prostředky a které by znamenalo zbavit vnitrostátní orgány cenného nástroje k zajišťování bezpečnosti státu; a

– trvalo pouze po dobu nezbytně nutnou k přijetí opatření umožňujících zhojit možnou neslučitelnost s unijním právem [104].

154. Pro toto řešení navíc hovoří obtížnost, kterou obnáší sladění vnitrostátních předpisů s judikaturou zavedenou ve věci Tele2 Sverige a Watson [105], a že vůle belgického zákonodárce dosáhnout souladu s rozsudkem Digital Rights byla zjevně vyjádřena upravením vlastních právních předpisů. Tento precedens naznačuje, že je také namístě sladit zákon ze dne 29. května 2016 (přijatý před tím, než byl vyhlášen rozsudek ve věci Tele2 Sverige a Watson) s judikaturou zavedenou tímto rozsudkem.

V. Závěry

155. Na základě výše uvedeného navrhuji, aby Soudní dvůr odpověděl Cour constitutionnelle (Ústavní soud, Belgie) 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 spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie musí být vykládán v tom smyslu, že:

– brání takové vnitrostátní právní úpravě, která provozovatelům a poskytovatelům služeb elektronických komunikací ukládá povinnost plošně a nerozlišujícím způsobem uchovávat provozní a lokalizační údaje všech účastníků a uživatelů v souvislosti se všemi prostředky elektronické komunikace;

– na výše uvedené nemá vliv, že cílem této vnitrostátní právní úpravy bylo nejen vyšetřování, odhalování a stíhání závažných nebo méně závažných trestných činů, nýbrž i národní bezpečnost, ochrana území, veřejná bezpečnost, předcházení zakázanému použití systémů elektronických komunikací, nebo kterýkoli jiný z cílů uvedených v čl. 23 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických

[104] – Rozsudek ze dne 28. února 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11; EU:C:2012:103), bod 62.

[105] – Bod 45 písemného vyjádření dánské vlády.

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);

– na výše uvedené nemá vliv ani to, že přístup k uchovávaným údajům podléhá přesně stanoveným zárukám. Předkládajícímu soudu přísluší, aby ověřil, zda vnitrostátní právní úprava podmínek tohoto přístupu ze strany příslušných orgánů omezuje tento přístup na zvláštní případy, jejichž závažnost činí zásah nezbytným, zda jej podmiňuje předchozím přezkumem (s výjimkou naléhavých případů) ze strany soudu nebo nezávislého orgánu, a zda stanoví, aby dotčené osoby byly o tomto přístupu vyrozuměny, pokud toto sdělení neznemožní jednání těchto orgánů.

2) Články 4 a 6 Listiny základních práv Evropské unie nemají dopad na výklad čl. 15 odst. 1 směrnice 2002/58 ve spojení s ostatními shora zmíněnými články Listiny v tom smyslu, že by bránily konstatování neslučitelnosti takové vnitrostátní právní úpravy, jako je úprava dotčená v původním řízení, s unijním právem.

3) Vnitrostátní soud může, pokud mu to vnitrostátní právo umožňuje, výjimečně a dočasně zachovat účinky takové právní úpravy, jako je úprava dotčená v původním řízení, a to navzdory její neslučitelnosti s unijním právem, pokud je toto zachování odůvodněno naléhavými důvody souvisejícími s hrozbami veřejné bezpečnosti nebo národní bezpečnosti, jimž by nebylo možno čelit jinými prostředky a jinými způsoby. Zachování těchto účinků bude moci trvat pouze po dobu nezbytně nutnou k nápravě zmíněné neslučitelnosti s unijním právem.“