

Věc C-520/18

**Shrnutí žádosti o rozhodnutí o předběžné otázce podle čl. 98 odst. 1
jednacího řádu Soudního dvora****Datum doručení:**

2. srpna 2018

Předkládající soud:

Cour constitutionnelle (Belgie)

Datum předkládacího rozhodnutí:

19. července 2018

Žalobci:

Ordre des barreaux francophones et germanophone

Académie Fiscale ASBL

UA

Liga voor Mensenrechten ASBL

Ligue des Droits de l'Homme ASBL

VZ

WY

XX

Žalovaná:

Conseil des ministres (belgická vláda)

I. Předmět a souvislosti původního řízení

- 1 Ordre des barreaux francophones et germanophone (Komora francouzsky a německy hovořících advokátů, dále jen „OBFG“), neziskové sdružení „Académie Fiscale“, neziskové sdružení „Liga voor Mensenrechten“, neziskové sdružení „Ligue des Droits de l'Homme“ a několik fyzických osob podaly ke

Cour constitutionnelle de Belgique [Ústavní soud (Belgie)] (dále jen „předkládající soud“) žalobu na neplatnost loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zákon ze dne 29. května 2016 o shromažďování a uchovávání údajů v odvětví elektronických komunikací, *Moniteur belge* ze dne 18. července 2016, s. 44717, dále jen „napadený zákon“). Tyto věci byly spojeny do jediného řízení.

- 2 Napadený zákon mění různá ustanovení loi du 13 juin 2005 relative aux communications électroniques (zákon ze dne 13. června 2005 o elektronických komunikacích, *Moniteur belge* ze dne 20. června 2005, s. 28070, dále jen „zákon ze dne 13. června 2005“), code d’instruction criminelle (dále jen „trestní řád“) a loi du 30 novembre 1998 organique des services de renseignement et de sécurité (organický zákon ze dne 30. listopadu 1998 o zpravodajských a bezpečnostních službách, *Moniteur belge* ze dne 18. prosince 1998, s. 40312, dále jen „zákon ze dne 30. listopadu 1998“).
- 3 Prostřednictvím loi du 30 juillet 2013, portant modification des articles 2, 126, et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l’article 90decies du Code d’instruction criminelle (zákon ze dne 30. července 2013 o změně článků 2, 126 a 145 zákona ze dne 13. června 2005 o elektronických komunikacích a článku 90j trestního řádu, *Moniteur belge* ze dne 23. srpna 2013, s. 56109, dále jen „zákon ze dne 30. července 2013“) belgické království částečně provedlo v belgickém právu směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (Úř. věst. 2006, L 105, s. 54), jakož i čl. 15 odst. 1 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (Úř. věst. 2002, L 201, s. 37; Zvl. vyd. 13/29, s. 514).
- 4 V rozsudku ze dne 8. dubna 2014, Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238) (dále jen „rozsudek Digital Rights Ireland a další“), Soudní dvůr prohlásil směrnici 2006/24 za neplatnou.
- 5 Předkládající soud rozsudkem č. 84/2015 ze dne 11. června 2015 zrušil článek 126 zákona ze dne 13. června 2005, ve znění zákona ze dne 30. července 2013, a to z týchž důvodů, jaké vedly Soudní dvůr k prohlášení neplatnosti směrnice 2006/24.
- 6 Belgický zákonodárce přijal napadený zákon s úmyslem reagovat na toto zrušení.

II. Předmět a právní základ žádosti o rozhodnutí o předběžné otázce

- 7 Napadený zákon mění zákon ze dne 13. června 2005, který provádí v belgickém právu několik směrnic včetně směrnice 2005/58.

III. Právní rámec předběžných otázek

1. Právo Evropské unie

A. Smlouva o EU

- 8 Článek 5 odst. 4 SEU stanoví:

„Podle zásady proporcionality nepřekročí obsah ani forma činnosti Unie rámec toho, co je nezbytné pro dosažení cílů Smluv.

Orgány Unie uplatňují zásadu proporcionality v souladu s Protokol o používání zásad subsidiarity a proporcionality.“

- 9 Článek 6 SEU stanoví:

„1. Unie uznává práva, svobody a zásady obsažené v Listině základních práv Evropské unie ze dne 7. prosince 2000, ve znění upraveném dne 12. prosince 2007 ve Štrasburku, jež má stejnou právní sílu jako Smlouvy.

Listina nijak nerozšiřuje pravomoci Unie vymezené ve Smlouvách.

Práva, svobody a zásady obsažené v Listině se vykládají v souladu s obecnými ustanoveními v hlavě VII Listiny, jimiž se řídí její výklad a použití, a s náležitým přihlédnutím k vysvětlením zmíněným v Listině, jež uvádějí zdroje těchto ustanovení.

2. Unie přistoupí k Evropské úmluvě o ochraně lidských práv a základních svobod. Přistoupení k této úmluvě se nedotkne pravomocí Unie vymezených Smlouvami. [...]“

B. Listina základních práv Evropské unie

- 10 Článek 4 Listiny stanoví:

„Zákaz mučení a nelidského či ponižujícího zacházení anebo trestu

Nikdo nesmí být mučen ani podroben nelidskému či ponižujícímu zacházení anebo trestu.“

- 11 Článek 6 Listiny stanoví:

„Právo na svobodu a bezpečnost

Každý má právo na svobodu a osobní bezpečnost.“

- 12 Článek 7 Listiny stanoví:

„Respektování soukromého a rodinného života

Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.”

13 Článek 8 Listiny stanoví:

„Ochrana osobních údajů

1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.“

14 Článek 11 Listiny stanoví:

„Svoboda projevu a informací

1. Každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice.

2. Svoboda a pluralita sdělovacích prostředků musí být respektována.“

15 Článek 47 Listiny stanoví:

„Právo na účinnou právní ochranu a spravedlivý proces

Každý, jehož práva a svobody zaručené právem Unie byly porušeny, má za podmínek stanovených tímto článkem právo na účinné prostředky nápravy před soudem.

Každý má právo, aby jeho věc byla spravedlivě, veřejně a v přiměřené lhůtě projednána nezávislým a nestranným soudem, předem zřízeným zákonem. Každému musí být umožněno poradit se, být obhajován a být zastupován.

Bezplatná právní pomoc je poskytnuta všem, kdo nemají dostatečné prostředky, pokud je to nezbytné k zajištění účinného přístupu ke spravedlnosti.“

16 Článek 52 Listiny stanoví:

„Rozsah a výklad práv a zásad

1. Každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení

zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.“ [...]

C. Směrnice 2002/58

- 17 Článek 15 odst. 1 směrnice 2002/58 stanoví:

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

D. Nařízení (EU) 2016/679

- 18 Článek 95 nařízení 2016/679 stanoví:

„Vztah ke směrnici 2002/58/ES

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

2. Vnitrostátní právo

- 19 Základní ustanovení relevantních vnitrostátních právních předpisů, ve znění napadeného zákona, jsou tato:

A. Zákon ze dne 13. června 2005 o elektronických komunikacích

- 20 Zákon ze dne 13. června 2005, ve znění napadeného zákona, stanoví:

„[...]“

Článek 126

1. Aniž je dotčen 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 vyhledávání, vyšetřování a stíhání trestných činů k provedení opatření stanovených v článcích 46a a 88a trestního řádu a za podmínek v nich stanovených;

2) zpravodajské a bezpečnostní služby za účelem plnění zpravodajských úkolů za použití metod sběru údajů uvedených v článcích 16/2, 18/7 a 18/8 [zákona ze dne 30. listopadu 1998] [...];

3) každý příslušník soudní policie a [belgického] Institutu [poštovních a telekomunikačních služeb] za účelem vyhledávání, vyšetřování a stíhání trestných činů spočívajících v 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 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 identifikace osoby, která zlovolně použila síť nebo službu elektronických komunikací [...]. 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.

Aniž jsou dotčena jiná právní ustanovení, 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 v pododstavcích 2 a 3, 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 jejich původu a místa určení, 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 pododstavcích 1 až 3, které mají být uchovávány, a požadavky, které musí tyto údaje splňovat.

4. K uchování 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 čl. 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 ohledně každé žádosti o poskytnutí těchto údajů ze strany orgánu uvedeného v odstavci 2.

Sledovatelnost stanovená v prvním pododstavci bodu 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.

[...]

Článek 126/1

1. U každého provozovatele a poskytovatele uvedeného v článku 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 46a, 88a a 90b trestního řádu a článků 18/7, 18/8, 18/16 a 18/17 [zákona ze dne 30. listopadu 1998].

[...].

Pouze členové Koordinační jednotky mohou odpovídat na žádosti orgánů o údaje uvedené v prvním pododstavci. Mohou si však pod svým dohledem a v rámci toho, co je naprosto nezbytné, obstarat technickou podporu od zaměstnanců provozovatele nebo poskytovatele.

Na členy Koordinační jednotky a na zaměstnance poskytující technickou podporu se vztahuje profesní tajemství.

Každý provozovatel a poskytovatel uvedený v čl. 126 odst. 1 prvním pododstavci zajistí důvěrnost údajů zpracovávaných Koordinační jednotkou a sdělí neodkladně Institutu a Komisi pro ochranu soukromí kontaktní údaje na Koordinační jednotku a její členy, jakož i každou změnu těchto údajů.

2. Každý provozovatel a 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 své odpovědi.

[...]

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

Tento pověřený zaměstnanec nesmí být členem Koordinační jednotky.

[...]

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

Plnění úkolů nesmí pro tohoto pověřeného zaměstnance představovat žádné znevýhodnění. Nesmí být konkrétně propuštěn nebo nahrazen ve funkci pověřeného zaměstnance z důvodu výkonu úkolů, které mu jsou svěřeny, bez důkladného odůvodnění.

Pověřený zaměstnanec musí mít možnost komunikovat přímo s vedením provozovatele nebo poskytovatele.

Zaměstnanec pověřený ochranou osobních údajů zajistí, aby:

- 1) zpracování prováděné Koordinační jednotkou bylo v souladu se zákonem;
- 2) poskytovatel nebo provozovatel shromažďoval a uchovával pouze údaje, které může legálně uchovávat;
- 3) pouze právem zmocněné orgány měly přístup k uchovávaným údajům;
- 4) byla provedena opatření na bezpečnost a ochranu osobních údajů popsaná v tomto zákoně a v bezpečnostní politice poskytovatele nebo provozovatele.

Každý poskytovatel a provozovatel uvedený v čl. 126 odst. 1 prvním pododstavci neprodleně sdělí Institutu a Komisi pro ochranu soukromí kontaktní údaje na zaměstnance pověřené ochranou osobních údajů, jakož i každou změnu těchto údajů.

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, 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) další 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.

Článek 127:

1. Král po konzultaci s Komisí pro ochranu soukromí a Institutem stanoví technická a administrativní opatření, která se ukládají provozovatelům, poskytovatelům uvedeným v čl. 126 odst. 1 prvním pododstavci nebo koncovým uživatelům, a to za účelem umožnění:

- 1) identifikace volající linky v případě tísňového volání;
- 2) identifikace koncového uživatele, vyhledání, lokalizace, odposlechu, zjištění a záznamu soukromých sdělení v souladu s podmínkami uvedenými v článcích 46a, 88a, 90b až 90j trestního řádu a v [zákoně ze dne 30. listopadu 1998].

[...]

2. Zakazuje se poskytovat nebo využívat službu nebo zařízení, které ztěžuje nebo znemožňuje provádění operací uvedených v odstavci 1, s výjimkou šifrovacích systémů, které lze použít za účelem zajištění důvěrnosti sdělení a bezpečnosti plateb.

[...]

Článek 145

1. Za porušení článků [...] 126, 126/1, 127 a vyhlášek přijatých k provedení článků [...] 126, 126/1 a 127 lze osobě uložit pokutu od 50 do 50 000 EUR.

[...]“.

B. Trestní řád

21 Trestní řád, ve znění napadeného zákona, stanoví:

„[...]“

Článek 46a

1. Při vyhledávání zločinů a přečinů 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 případech krajní naléhavosti může každý příslušník soudní policie s písemným a předchozím 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, které nemohou vést k trestu odnětí svobody jako hlavnímu trestu na jeden rok nebo k přísnějšímu trestu, 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, aby sdělil údaje uvedené v prvním odstavci, předá státnímu zástupci nebo příslušníkovi soudní policie údaje, o něž byl požádán, ve lhůtě, kterou stanoví král [...]

[...]

Každá osoba, která vzhledem ke své funkci ví o opatření nebo v rámci opatření poskytuje svou součinnost, je povinna zachovávat tajemství. Každé porušení tohoto tajemství se trestá v souladu s článkem 458 trestního zákoníku.

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

Článek 88a

1. V případě, že existují přesvědčivé indicie, že trestné činy mohou vést k trestu odnětí svobody jako hlavnímu trestu na jeden rok nebo k přísnějšímu trestu, a má-li vyšetřující soudce za to, že existují okolnosti, které vyžadují za účelem zjištění pravdy vyhledat elektronická sdělení nebo lokalizovat původ nebo místo určení 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 původu nebo místa určení elektronických sdělení.

V případech uvedených v prvním pododstavci se pro každý elektronický komunikační prostředek, jehož údaje o hovoru se vyhledávají nebo jehož původ nebo místo určení telekomunikace se lokalizují, v protokolu zaznamená den, hodina, doba trvání a v případě nutnosti 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 moct 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 ze dne 13. června 2005 o elektronických komunikacích, použijí se následující ustanovení:

- u trestného činu uvedeného v knize II hlavě Ib trestního zákoníku si může vyšetřující soudce v usnesení vyžádat údaje za dobu dvanácti měsíců před usnesením;

- u jiného trestného činu uvedeného v čl. 90b odst. 2 až 4, který není uveden v první odrážce, u trestného činu, který je spáchán v rámci zločinecké skupiny uvedené v článku 324a trestního zákoníku, nebo u trestného činu, který může vést k trestu odnětí svobody jako hlavnímu trestu na pět let nebo k přísnějšímu trestu, 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 přesné 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 provinční lékařské komory, v závislosti na konkrétním případě. Vyšetřující soudce sdělí týmž osobám skutečnosti, které se podle něj vztahují k profesnímu tajemství. Tyto skutečnosti nejsou zaznamenány v protokolu. [...] Každá osoba, která vzhledem ke své funkci ví o opatření nebo v rámci opatření poskytuje svou součinnost, je povinna zachovávat tajemství. Každé porušení tohoto tajemství se trestá v souladu s článkem 458 trestního zákoníku.

[...]“

C. Zákon ze dne 30. listopadu 1998

22 Zákon ze dne 30. listopadu 1998, ve znění napadeného zákona, stanoví:

„[...]“

Článek 13

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

Informace obsažené v záznamech musí být spojeny 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. [...]

Článek 18/3

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 případě 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 bodem 2 a 3;
- 5) doba, po kterou lze zvláštní metodu použít ode dne oznámení rozhodnutí Komisi;
- [...]
- 9) případně přesvědčivé 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. Vedoucí služby ukončí použití zvláštní metody, 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. [...]

Článek 18/8

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 původu nebo místa určení elektronických sdělení.

[...]

2. Pokud jde o použití metody uvedené v odstavci 1 na údaje uchovávané na základě článku 126 zákona ze dne 13. června 2005 o elektronických komunikacích, použijí se následující ustanovení:

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

IV. Další ustanovení a zásady, kterých se dovolávají účastníci řízení nebo které uvádí odůvodnění rozhodnutí předkládajícího soudu

23 Kromě výše uvedených ustanovení to jsou následující ustanovení a zásady, kterých se dovolávají účastníci řízení nebo které uvádí odůvodnění rozhodnutí předkládajícího soudu:

- Články 5, 6, 8, 9, 10, 11, 14, 15, 17 a 18 Evropské úmluvy o ochraně lidských práv a základních svobod, podepsané v Římě dne 4. listopadu 1950 (dále jen „EULP“)
- článek 17 Mezinárodního paktu o občanských a politických právech, uzavřeného v New Yorku dne 16. prosince 1966 (dále jen „Pakt“)
- článek 2 písm. a) a čl. 13 odst. 1 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. 1995, L 281, s. 31; Zvl. vyd. 13/15, s. 335);

- články 10, 11, 12, 15, 19, 22 a 29 a čl. 151 odst. 1 první pododstavec belgické ústavy;
- obecné zásady právní jistoty, proporcionality, zákonnosti v trestních věcech, přiměřenosti, presumpce nevinny, práva na spravedlivý proces, profesního tajemství, rovnosti mezi občany a informačního sebeurčení.

VI. Hlavní argumenty účastníků řízení

1. Žalobní důvody uplatňované žalobci

- 24 Žalobci namítají porušení několika článků Ústavy, a to samostatně nebo ve spojení s několika články Smlouvy o EU, Listiny, směrnice 2002/58 a dalšími ustanoveními unijního práva, společně s několika ustanoveními EÚLP, článkem 17 Paktu a s obecnými právními zásadami.
- 25 Napadený zákon ukládá provozovatelům elektronických komunikací plošnou povinnost uchovávat po určitou dobu provozní a lokalizační údaje uživatelů. Napadený zákon rovněž stanoví režim přístupu soudních orgánů a zpravodajských a bezpečnostních služeb k těmto údajům.
 - *K povinnosti shromažďovat a uchovávat údaje*
- 26 Žalobci namítají, že napadený zákon neodůvodněně zachází stejným způsobem s uživateli telekomunikačních služeb či služeb elektronických komunikací, na které se vztahuje profesní tajemství, mimo jiné s advokáty, a s ostatními uživateli těchto služeb, aniž je zohledněno zvláštní postavení advokáta, význam profesního tajemství, kterým je vázán, a nezbytnost vztahu důvěry, který musí mít se svými klienty, či zvláštní postavení účetních a daňových poradců, význam profesního tajemství, kterým jsou vázáni, nezbytnost vztahu důvěry, který musí mít se svými klienty, či povinnost zachovávat důvěrnost, jež mají další osoby, které nejsou vázány profesním tajemstvím v úzkém smyslu.
- 27 Diskriminační situace, kterou vytváří napadený zákon, je na újmu advokátům i jednotlivcům, neboť profesní tajemství advokátů je věcí obecného zájmu. Všechny osoby, které se s důvěrou obrátí na advokáta, musí mít jistotu, že uskutečnění a okolnosti této porady ani tajemství sdělená jejich právnímu poradci nebudou vyzrazeny ani uplatněny vůči nim. Zásada profesního tajemství advokátů se přímo dotýká práva na spravedlivý proces a práva na respektování soukromého života. Může do něj tedy být zasaženo pouze ve výjimečných případech, a to za dodržení odpovídajících a dostatečných záruk proti zneužití.
- 28 Přestože se získané údaje netýkají obsahu sdělení, umožňují sestavit skutečný digitální průkaz totožnosti dotčené osoby. Bude tak možné určit, zda osoba podezřelá ze spáchání trestného činu kontaktovala advokáta, a zjistit den, hodinu a délku komunikace, jakož i komunikační zařízení uživatelů, místo použití

mobilního komunikačního prostředku atd. Tyto údaje jsou ještě přesnější než údaje obsažené v pracovním diáři advokáta, který je však důvěrným dokumentem.

- 29 Nerozlišování mezi osobami, na jejichž sdělení se vztahuje profesní tajemství, a ostatními osobami bylo předmětem kritiky Soudního dvora v rozsudku ze dne 21. prosince 2016, Tele2 Sverige a Watson a další (C-203/15 a C-698/15, EU:C:2016:970) (dále jen „rozsudek Tele2 Sverige a Watson a další“).
- 30 Z technického hlediska by bylo jednoduché vytržít běžná metadata a metadata vztahující se k nositeli povinnosti profesního tajemství, a to prostřednictvím vstupního filtrovacího mechanismu. Zákonodárce by totiž mohl přinutit provozovatele, aby zohlednili to, že jejich klienti jsou nositeli povinnosti profesního tajemství, a aby tuto informaci mezi sebou sdíleli. Provozovatelé by tedy do vytvořených databází nevkládali metadata vztahující se na sdělení advokátů a jiných nositelů povinnosti profesního tajemství.
- 31 Není navíc stanoven žádný kontrolní mechanismus, který by umožnil nositelům povinnosti profesního tajemství a osobám, v jejichž prospěch je stanoveno, bránit se vůči shromažďování, uchovávání a zjištění údajů, na které se vztahuje profesní tajemství. Toto zjištění údajů přitom stačí k tomu, aby došlo k zásahu do profesního tajemství, přestože tyto údaje poté nejsou použity ve spisu. Práva zaručená článkem 6 EÚLP a článkem 47 Listiny nejsou dodržena, jelikož napadený zákon nestanoví žádnou soudní kontrolu.
- 32 Kromě toho napadená ustanovení zachází stejným způsobem s jednotlivci, kteří jsou předmětem vyšetřovacích úkonů nebo stíhání ohledně skutečností, které mohou vést k odsouzení v trestním řízení, a jednotlivci, kteří nejsou předmětem takových úkonů. Trestní právo je přitom založeno na zásadě presumpce nevin, jejímž logickým důsledkem je to, že důkazní břemeno nese státní zastupitelství a v pochybnostech se rozhodne ve prospěch obviněného. Nebylo by tedy relevantní dovolávat se skutečnosti, že opatření může být také ku prospěchu oběti trestného činu. V tomto ohledu jdou povinnosti uchovávat údaje, které stanoví napadený zákon, nad rámec cílů zákonodárce.
- 33 Plošné uchovávání údajů, a to včetně údajů ohledně osob, které nejsou nijak spojeny s trestnou činností, tedy porušuje zásadu proporcionality. Toto porušení je potvrzeno rozsudky Soudního dvora Digital Rights Ireland a další a Tele2 Sverige a Watson a další, jakož i stanoviskem generálního advokáta Cruz Villalóna ve spojených věcech Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2013:845) i rozsudkem předkládajícího soudu č. 84/2015 ze dne 11. června 2015.
- 34 Plošná a nerozlišující povinnost uchovávat identifikační údaje, údaje o připojení, lokalizační údaje a údaje o osobní komunikaci, kterou stanoví napadený zákon, představuje rovněž zásah do práva na ochranu soukromí, který není v demokratické společnosti naprosto nezbytný pro zajištění národní bezpečnosti, tj. bezpečnosti státu, národní obrany, veřejné bezpečnosti nebo pro prevenci,

vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/46.

- 35 V rozsudku Tele2 Sverige a Watson a další Soudní dvůr prohlásil, že unijní právo brání vnitrostátní právní úpravě, která stanoví plošné a nerozlišující uchovávání údajů. I za předpokladu, že takovou plošnou povinnost uchovávat údaje nelze samu o sobě považovat za přesahující meze toho, co je naprosto nezbytné, musí v každém případě zahrnovat veškeré záruky uvedené Soudním dvorem v rozsudku Digital Rights Ireland a další a v rozsudku Tele2 Sverige a Watson a další. Tyto záruky jsou imperativní, kumulativní a minimální (stanovisko generálního advokáta Saugmandsgaarda Øe ve spojených věcech Tele2 Sverige a další, C-203/15 a C-698/15, EU:C:2016:572).
- 36 Povinnost uchovávat údaje stanovená napadeným zákonem do velké míry odpovídá povinnosti uchovávat údaje, která byla stanovena směrnicí 2006/24, jak konstatoval Soudní dvůr v bodě 97 rozsudku Tele2 Sverige a Watson a další.
- 37 Plošná povinnost uchovávat údaje stanovená napadeným zákonem tedy představuje obzvláště závažný zásah do práva na respektování soukromého a rodinného života a do práva na ochranu osobních údajů. Má rovněž dopad na používání prostředků elektronické komunikace, a tedy na způsob, jakým uživatelé těchto komunikačních prostředků uplatňují svou svobodu projevu. Z toho rovněž plyne porušení ustanovení mezinárodního a ústavního práva, která tuto svobodu projevu zaručují. Vzhledem k závažnosti zásahu do těchto základních práv by toto opatření mohl odůvodnit pouze boj proti závažné trestné činnosti. Boj proti závažné trestné činnosti přitom nemůže sám o sobě odůvodnit plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů (rozsudek Tele2 Sverige a Watson a další, bod 103). Znamenalo by to totiž, že uchovávání těchto údajů se stane pravidlem, ačkoliv podle směrnice 2002/58 je pravidlem zákaz uchovávání těchto údajů, zatímco jejich uchovávání je výjimkou. Kromě toho rozsudek Tele2 Sverige a Watson a další se týká veškeré vnitrostátní právní úpravy boje proti trestné činnosti, která stanoví plošnou povinnost uchovávat údaje, a nikoli pouze boje proti závažné trestné činnosti. I když může být každý občan konfrontován s tímto druhem trestné činnosti jako obviněný, oběť nebo svědek, dotčená právní úprava spadá do oblasti působnosti článku 15 směrnice 2002/58. Rozsudek Tele2 Sverige a Watson a další se na ni tedy uplatní.
- 38 V rozsudku Tele2 Sverige a Watson a další Soudní dvůr uvedl, že vnitrostátní právní úprava, jež umožňuje cílené preventivní uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti, může být přípustná v míře nezbytně nutné uvedené v tomto rozsudku. Zákonodárce v rámci přípravných prací uvedl, že takové cílené uchovávání by nebylo možné. Argumentace belgického státu ve skutečnosti spočívá na politické vůli pokračovat za každou cenu v plošném uchovávání údajů pod záminkou existence hrozby teroristických útoků a navzdory protiústavnosti plošného systému monitorování, který byl zaveden. I kdyby skutečně nebylo možné předem určit kategorie osob,

kterých se nemohou týkat závažné trestné činy nebo které do nich nemohou být zapojeny, neumožňovalo by to odůvodnit natolik závažný zásah do soukromí občanů. Logickým důsledkem by mělo být, že takové opatření nebude zavedeno.

- 39 I když konečně důvodová zpráva k zákonu poukazuje na význam komunikačních údajů pro vyšetřování terorismu, dětské pornografie, podezřelých zmizení, nelegálního obchodu s omamnými látkami, prodeje padělaných léků na internetu, podněcování k nenávisti nebo násilí, obtěžování, zneužití bankovních účtů a krádeží identity, několik studií nezbytnost plošné povinnosti uchovávat údaje za účelem boje proti závažné trestné činnosti zpochybňuje (stanovisko generálního advokáta Saugmandsgaarda Øe ve spojených věcech Tele2 Sverige a další, C-203/15 a C-698/15, EU:C:2016:572).
- 40 Podpůrně účastníci řízení tvrdí, že rozsudek Digital Rights Ireland a další lze vykládat dvěma způsoby: podle jednoho výkladu protiprávnost plošné a nerozlišující povinnosti uchovávat údaje vyplývá z absence dostatečných záruk ohledně přístupu k uchovávaným údajům a doby uchovávání; podle druhého výkladu je povinnost uchovávat údaje protiprávní právě z důvodu své plošné a nerozlišující povahy. Důvodová zpráva k zákonu rovněž uznává, že plošná a nerozlišující povinnost uchovávat údaje není v souladu s tímto rozsudkem, ale uvádí, že to může být vyváжено striktnější právní úpravou jiných aspektů, a sice rozlišováním mezi kategoriemi uchovávaných údajů a jejich užitečností, pravidly přístupu orgánů k dotčeným údajům a pravidly v oblasti bezpečnosti údajů u provozovatelů. Je tedy třeba konstatovat, že plošná povinnost uchovávat údaje neodpovídá ani volnému výkladu tohoto rozsudku, a to z důvodu absence záruk za účelem omezení zásahu na to, co je nezbytně nutné.
- 41 Je sice pravda, že provozovatelé uchovávají údaje pro účely fakturace. Napadený zákon jim však zakazuje používat údaje uchovávané podle tohoto zákona k jiným účelům než těm stanoveným zákonem, a tedy i k fakturaci svých služeb. Napadený zákon jim kromě toho ukládá uchovávat údaje, které by neuchovávaly, nikoli v této podobě a v každém případě ne po takto dlouhou dobu.
- 42 Existuje dále nezanedbatelné riziko, že příslušné databáze budou spravovány nerozvázně ze strany provozovatelů, kteří se zdráhají kontroly, která je spojena s touto novou povinností.
- 43 Žádný nezávislý orgán nekontroluje dodržování úrovně zajištění a ochrany uchovávaných údajů ze strany provozovatelů. Všechny odpovědné osoby určené v tomto ohledu napadeným zákonem jsou zaměstnanci provozovatelů, kteří se nacházejí v podřízeném postavení.
- 44 Napadený zákon navíc provozovatelům umožňuje předat údaje shromážděné pro účely uchovávání a zpracování zpracovatelem do jiných členských států Evropské unie navzdory citlivé a důvěrné povaze určitých údajů, což podstatně zvyšuje riziko, že k nim získají přístup třetí osoby nebo že budou zpřístupněny. Vnitrostátní právní úpravy v jiných členských státech, například francouzské

právní předpisy, navíc umožňují zpravodajským službám získat od provozovatelů informace o údajích, s nimiž tito provozovatelé zachází.

– ii) *K době uchování*

- 45 Pokud jde o dobu uchovávání údajů, napadený zákon v podstatě stanoví dobu dvanácti měsíců, což je samo o sobě nepřiměřené. Je sice pravda, že u trestných činů, které nemohou vést k odnětí svobody jako hlavnímu trestu na jeden rok nebo na delší dobu, se mohou vyžadované údaje týkat pouze šesti měsíců před podáním žádosti. Těchto trestných činů je však málo.
- 46 Počátky běhu doby uchovávání ani nejsou závislé na okolnostech, které případně odůvodňují toto uchování. Identifikační údaje mohou být ostatně *de facto* uchovávány po mnohem delší dobu než dvanáct měsíců, neboť doba uchovávání počíná běžet ode „dne, kdy je komunikace prostřednictvím používané služby naposledy možná“.
- 47 Jiné evropské země uplatňují kratší doby uchovávání. Odkazuje se na rozsudek německého ústavního soudu, který zrušil německý zákon o uchovávání údajů, jakož i na rozsudek Digital Rights Ireland a další.
- 48 Doby uchovávání údajů lze rovněž kritizovat z toho důvodu, že je stejná pro všechny kategorie údajů, ačkoliv by měla být rozlišena podle kategorií údajů, jejich užitečnosti s ohledem na sledovaný cíl nebo podle dotčených osob, a to za předpokladu, že je omezena na to, co je nezbytně nutné. Toto stejné zacházení s rozdílnými kategoriemi uchovávaných údajů není rozumně odůvodněné, a je tudíž diskriminační.
- 49 Konečně napadený zákon neukládá orgánu, který získal přístup k údajům, aby tyto údaje zničil, pokud nijak nesouvisí s cílem, pro který byly shromážděny, nebo pokud již nejsou nezbytně nutné k boji proti závažné trestné činnosti.

– iii) *K přístupu k údajům*

- 50 Napadený zákon umožňuje získat přístup k uchovávaným údajům šesti různým orgánům namísto toho, aby tento přístup omezil striktně jen na orgány, které se podílejí na boji proti trestné činnosti, přinejmenším proti závažné trestné činnosti.
- 51 Napadený zákon umožňuje orgánům získat přístup k uchovávaným údajům, aniž je tento přístup omezen na závažnou trestnou činnost. Doplnkové záruky stanovené napadeným zákonem v oblasti profesního tajemství se netýkají jiných osob, na které se vztahuje profesní tajemství, než jsou advokáti, lékaři a novináři. Článek 458 trestního zákoníku [ustanovení, které ukládá dodržování profesního tajemství] se přitom vztahuje i na další osoby než ty, které vykonávají tato tři povolání. Na některé osoby, orgány a organizace se navíc nevztahuje profesní tajemství, ačkoliv důvěrnost komunikace s nimi musí být v jistém rozsahu

chráněna podle jiných ustanovení. Státní zástupce mimoto není soudním orgánem ani nezávislým správním orgánem.

- 52 Napadený zákon umožňuje získat přístup k uchovávaným údajům mimo jiné zpravodajským a bezpečnostním službám. Oblast působnosti těchto služeb byla vymezena příliš široce. Komunikační údaje všech občanů mohou být vyžadovány po dobu šesti, devíti nebo dvanácti měsíců před rozhodnutím o přístupu v závislosti na povaze možné hrozby. Napadený zákon tedy může vést ke zneužití pravomoci na úkor jednotlivců nebo organizací s kritickými postoji vůči vládě či politickému systému. Svoboda tisku je rovněž ohrožena tím, že zpravodajské a bezpečnostní služby si mohou vyžádat veškerá telefonická a internetová sdělení novinářů. Napadený zákon by mohl rovněž vyvolat nebo posílit autocenzuru občana, který má neurčitý dojem, že je sledován, což může mít dopad na výkon jeho svobody zastávat názory a svobody informací, a představovat tudíž zásah ve smyslu článku 11 Listiny.
- 53 Neexistuje žádný podrobný popis okolností ani podmínek pro poskytnutí přístupu. Na přístup se ani nevztahují žádné hmotněprávní či procesní podmínky, jelikož poskytovatelé jsou jednoduše povinni vyhovět všem žádostem šesti určených orgánů. V rozsudku Tele2 Sverige a Watson a další přitom Soudní dvůr prohlásil, že vnitrostátní právní úprava musí stanovit odpovídající záruky, tj. jasná a přesná pravidla, která vymezují okolnosti a podmínky, za nichž musí poskytovatelé poskytnout příslušným vnitrostátním orgánům přístup. Tentýž rozsudek upřesňuje, že přístup lze v zásadě udělit 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. Dále je třeba, aby přístup podléhal přechozí kontrole ze strany soudu nebo nezávislého správního orgánu. Napadený zákon přitom nestanoví žádná procesní pravidla a neurčuje ani žádný orgán, který by posuzoval žádost o poskytnutí údajů. Jediné stanovené kontroly jsou kontroly *a posteriori*.
- 54 Dále pak rozsudek Tele 2 Sverige a Watson a další používá pojem „závažné ohrožení veřejné bezpečnosti“. Napadený zákon přitom toto kritérium nezachovává, neboť se týká běžných a specifických metod zpravodajských služeb a tyto se vztahují na méně závažná narušení bezpečnosti než metody zvláštní.
- 55 Konečně napadený zákon neukládá žádnou povinnost sdělit osobám, že byl udělen přístup k jejím soukromým údajům, což tyto osoby rovněž zbavuje práva na skutečný a účinný opravný prostředek.
- 56 Pokud jde o dobu přístupu, zákon stanoví odlišnou úpravu pouze v závislosti na druhu trestného činu a hrozby, ale nikoli v závislosti na druhu uchovávaných údajů.

2. Důvody uplatňované belgickým státem v rámci obrany

- 57 Rada ministrů má za to, že napadený zákon odpovídá na kritiku Soudního dvora a předkládajícího soudu ohledně dřívější použitelné právní úpravy.
- 58 Přestože je profesní tajemství advokáta záležitostí veřejného pořádku, není absolutní. Zásada proporcionality „musí umožňovat posoudit meze plynoucí ze zásady nezbytnosti či jiných zásad nebo hodnot, které jsou případně v kolizi s tímto profesním tajemstvím“.
- 59 Pokud jde o přístup k údajům, napadený zákon stanoví meze týkající se profesního tajemství, a to zejména profesního tajemství advokáta. Zákon se vztahuje pouze na metadata, a nikoli na obsah sdělení. Není jím tedy skutečně dotčena důvěrnost vzájemných sdělení advokáta a jeho klienta. Bylo by naopak nepřiměřené zcela vyloučit z právní úpravy sdělení pocházející od příslušníků profesí, na které se vztahuje profesní tajemství, a sdělení jím určená. To, že je e-mailová adresa používána osobou, na kterou se vztahuje profesní tajemství, totiž ještě neznamená, že všechny zprávy, které byly zaslány na tuto adresu nebo z této adresy, jsou skutečně chráněny profesním tajemstvím. Osoby, na které se vztahuje profesní tajemství, mohou samy páchat závažné trestné činy.
- 60 Ve vztahu k jednotlivcům, kteří by se již nemohli s důvěrou obracet na svého advokáta, přijal zákonodárce veškerá opatření, aby mohlo být dosaženo sledovaného cíle, jehož legitimita není zpochybňována, bez nepřiměřeného zásahu do práva na soukromí a práva na spravedlivý proces.
- 61 Pokud jde o uchovávání údajů podle toho, zda se na dotyčnou osobu vztahuje profesní tajemství či nikoli, přípravné práce k zákonu poukázaly na technické obtíže takového přístupu a na skutečnost, že ostatním členským státům Unie se nepodařilo najít technické řešení pro rozlišování. Kromě toho by takové rozlišování nechránilo ani tak profesní tajemství jako takové, ale spíše osobu, která v rámci svého povolání uchovává tajemství. Toto rozlišování by vedlo k tomu, že by bylo z působnosti zákona vyloučeno to, na co se vztahuje profesní tajemství, ale rovněž to, na co se profesní tajemství vůbec nevztahuje, a to pod záminkou, že shromážděné informace jsou přenášeny stejnými prostředky jako informace, na které se profesní tajemství vztahuje.
- 62 Pokud jde o nemožnost podat opravný prostředek proti rozhodnutí, kterým se ukládá zpřístupnění uchovávaných údajů, jakož i proti opatřením přijatým na základě tohoto rozhodnutí, je přístup k uchovávaným údajům ve skutečnosti předmětem soudního přezkumu v rámci trestního vyšetřování, který vykonává Komise BIM [Správní komise odpovědná za dohled nad specifickými a výjimečnými metodami shromažďování údajů ze strany zpravodajských a bezpečnostních služeb], složená z nezávislých soudců, pokud se jedná o zpravodajské služby, které získávají přístup k informacím. Sám státní zástupce má nezávislé postavení při výkonu svých vyšetřovacích pravomocí v rámci

trestního řádu a zaručuje, že výkon jeho pravomocí nebude nepřiměřeně zasahovat do práva na ochranu soukromí.

- 63 Pokud jde o dobu uchovávání údajů, podle zákona je přístup odstupňován v podstatě na základě závažnosti trestného činu. Přístupu k uchovávaným informacím logicky předchází povinnost je uchovávat. Pouze žádost o přístup umožní určit závažnost trestného činu nebo hrozby. Vzhledem k tomu, že se podle zákona přístup k dotyčným informacím odvíjí od závažnosti trestného činu nebo hrozby, je obtížné předem určit, které kategorie informací budou užitečné pro konkrétní vyšetřování. Konečně žalobce neuvádí, proč jsou podle něj doby stanovené zákonem samy o sobě nepřiměřené.
- 64 Zákonodárce posoudil všechny možnosti, jak vyhovět požadavkům judikatury Soudního dvora. Rozdílné zacházení z hlediska doby uchovávání údajů bylo po důkladném zvážení této otázky posouzeno jako nemožné. Ukázalo se, že doba dvanácti měsíců je nezbytná k boji proti teroristickým trestným činům.
- 65 K tomu, že se mezi jednotlivci nerozlišuje podle toho, zda jsou předmětem vyšetřování nebo stíhání, lze uvést, že právní úprava v napadeném zákoně právě vyšetřovatelům umožňuje získat přístup k určitým metadatům týkajícím se osoby, která je předmětem takového vyšetřování. To předkládá, že tato metadata byla uchována před tímto šetřením, a tedy v době, kdy nebylo možné rozlišení provést.
- 66 Pokud jde o riziko, že provozovatelé budou údaje, které byly uchovány, zpracovávat nerozváženě, platí, že dodržování právních povinností provozovatelů kontroluje regulační orgán daného odvětví, přičemž tato kontrola je spojena se sankcemi, které mohou spočívat i v odnětí licence. Napadený zákon stanoví četné záruky v oblasti zajištění údajů.
- 67 Žádný jiný preventivní systém by nemohl zabránit tomu, aby byly údaje, na které se vztahuje profesní tajemství, uchovávány a aby k nim byl případně umožněn přístup. K určení, zda se na určitou informaci vztahuje profesní tajemství, je nutně třeba ji předem zpracovat.
- 68 Cílem vnitrostátních právních předpisů ve Švédsku a ve Spojeném království, kterými se zabýval Soudní dvůr v rozsudku Tele2 Sverige a Watson a další, byl boj proti závažné trestné činnosti, zatímco napadený zákon si stanovil širší cíl. V důsledku toho nelze závěr Soudního dvora o nevhodnosti či nepřiměřenosti vnitrostátních právních předpisů ve vztahu k cíli boje proti závažné trestné činnosti obdobně vztáhnout na vnitrostátní právní předpisy, které sledují odlišný cíl.
- 69 Je sice pravda, že Soudní dvůr rozhodl, že právní úprava, která by umožňovala shromažďování, uchovávání a přístup příslušných vnitrostátních orgánů k údajům týkajícím se elektronických komunikací, by nebyla v rozporu s unijním právem, kdyby byla tato právní úprava cílená. Tato možnost uznaná Soudním dvorem je však jen teoretická. Soudní dvůr totiž v tomto rozsudku nezkoumal soulad

konkrétní právní úpravy, která by byla takto cílená. Je přitom sporné, zda může být takový systém zaveden, aniž by znamenal porušení zásady rovnosti občanů.

- 70 Z přípravných prací vyplývá, že cíl napadeného zákona se liší od konkrétní situace, kterou zkoumal Soudní dvůr v rozsudcích ve věcech Digital Rights Ireland a další a Tele2 Sverige a Watson a další. V těchto rozsudcích totiž musel Soudní dvůr rozhodnout o otázce, zda byla plošná a nerozlišující povinnost uchovávat údaje nezbytná a přiměřená ve vztahu k boji proti závažné trestné činnosti. Napadený zákon přitom sleduje jiný cíl. Jedná se o zajištění integrity systému trestního soudnictví a zvýšení důvěry občanů ve fungování soudnictví prostřednictvím nalezení pravdy v zájmu oběti, obviněného a všech ostatních dotčených osob.
- 71 Mezi plošnou povinností uchovávat údaje a cílem sledovaným zákonodárcem existuje vztah přiměřenosti, který je kromě toho zcela v souladu s čl. 15 odst. 1 směrnice 2002/58. I když každý občan není potenciálním zločincem, každý občan totiž může být konfrontován s trestnou činností, ať už jako oběť, obviněný nebo svědek, a má tedy zájem na nalezení pravdy. Navzdory obecné povinnosti uchovávat údaje jsou zavedeny záruky nezbytné pro ochranu soukromí, a to z hlediska uchovávání těchto údajů a z hlediska přístupu k nim. S ohledem na tyto záruky nemá povinnost uložená zákonem nepřiměřenou povahu. Napadený zákon není v rozporu s judikaturou Soudního dvora.
- 72 Bylo rozhodnuto, že dřívější právní předpisy nepřiměřeně zasahovaly do práva na respektování soukromého života z důvodu kombinace čtyř prvků: skutečnost, že uchovávání údajů se vztahovalo na všechny osoby, nerozlišování v závislosti na kategoriích uchovávaných údajů a jejich užitečnosti, neexistence či nedostatečnost pravidel, což představovalo porušení práva na ochranu soukromí.
- 73 Soudní dvůr ani předkládající soud přitom neměly za to, že jeden z těchto čtyř prvků může postačovat k závěru, že opatření je nepřiměřené. Kontrola zásady proporcionality totiž předpokládá komplexní přístup. Plošnou povinnost uchovávat údaje doprovází dostatečné záruky ohledně přístupu k údajům, dob uchovávání a ochrany a bezpečnosti údajů, a to tak, že je zásah omezen na to, co je nezbytně nutné.
- 74 Napadený zákon je v souladu s čl. 15 odst. 1 směrnice 2002/58, a to i jde-li o uchovávání údajů a jejich předávání příslušným orgánům za účelem vyšetřování a stíhání jiných forem trestné činnosti, než je závažná trestná činnost, je-li ohrožen život nebo fyzická integrita osob nebo věcí, nebo jsou-li neoprávněně použity systémy elektronických komunikací.
- 75 Rozsudek Tele2 Sverige a Watson a další neukládá, aby měly záruky kumulativní povahu, a nijak toto konstatování nezpochybňuje.
- 76 Belgický stát nakonec odkazuje na přípravné práce k napadenému zákonu.

VII. Stručné odůvodnění žádosti o rozhodnutí o předběžné otázce

- 77 Dřívější první předpisy, které má napadený zákon nahradit, byly zrušeny předkládajícím soudem v rozsudku č. 84/2015 ze dne 11. června 2015, jehož odůvodnění je široce citováno v této žádosti o rozhodnutí o předběžné otázce. Tento rozsudek je dostupný na internetových stránkách belgického ústavního soudu: <http://www.const-court.be/public/f/2015/2015-084f.pdf>.
- 78 Předkládající soud dále cituje přípravné práce k zákonu (Doc. parl. Cahmbre, 2015–2016, 54–1567), které jsou k dispozici na adrese <https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=54&dossierID=1567>.
- 79 Předkládající soud zdůrazňuje, že z přípravných prací k napadenému zákonu vyplývá, že zákonodárce důkladně posoudil jeho výše uvedený rozsudek č. 84/2015 ze dne 11. června 2015 i rozsudek Soudního dvora ve věci Tele2 Sverige a Watson a další, na němž je založen.
- 80 Vyplývá z nich, že cílem, který zákonodárce sleduje v napadeném zákoně, je nejen boj proti terorismu a dětské pornografii, ale také možnost použít uchovávané údaje v široké škále situací, kdy tyto údaje mohou být výchozím bodem, ale i jednou z fází trestního vyšetřování.
- 81 Zákonodárce měl za to, že je s ohledem na sledovaný cíl nemožné zavést cílenou a rozlišující povinnost uchovávat údaje a že se rozhodl spojit plošnou a nerozlišující povinnost uchovávat údaje se striktními zárukami, a to jak z hlediska ochrany uchovávání, tak z hlediska přístupu, aby byl co nejvíce omezen zásah do práva na respektování ochrany soukromého života. V této souvislosti bylo zdůrazněno, že je jednoduše nemožné předem rozlišovat z hlediska osob, časových období a zeměpisných oblastí. Tato nemožnost byla podrobně vyložena v přípravných pracích (viz dokument 1, body 7 až 10, <http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf>).
- 82 V rozsudku ze dne 21. prosince 2016, Tele2 Sverige a Watson a další (C-203/15 a C-698/15, EU:C:2016:970), tj. po přijetí napadeného zákona, Soudní dvůr odpověděl na dvě předběžné otázky týkající se výkladu čl. 15 odst. 1 směrnice 2002/58.
- 83 Soudní dvůr v bodě 78 tohoto rozsudku dospěl k závěru, že „se legislativní opatření, jehož prostřednictvím členský stát ukládá na základě čl. 15 odst. 1 směrnice 2002/58 poskytovatelům služeb elektronických komunikací, aby pro účely uvedené tímto ustanovením udělili za podmínek stanovených takovým opatřením přístup k údajům uchovávaným uvedenými poskytovateli, týká zpracování osobních údajů ze strany uvedených poskytovatelů, na které se vztahuje oblast působnosti této směrnice“.
- 84 Soudní dvůr připomíná, že v čl. 5 odst. 1 směrnice se stanoví, že členské státy musí prostřednictvím svých vnitrostátních právních předpisů zajistit důvěrný

charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů. Zásada důvěrnosti vyžaduje, že se třetím osobám zakazuje uchovávat bez souhlasu uživatelů provozní údaje související s jejich elektronickými sděleními (body 84 a 85).

- 85 Soudní dvůr rovněž připomíná, že čl. 15 odst. 1 směrnice umožňuje členským státům zavést výjimky ze základní povinnosti stanovené v čl. 5 odst. 1, přičemž tyto výjimky musí být v souladu s ustálenou judikaturou Soudního dvora vykládány striktně. „[Článkem 15] tudíž nemůže být odůvodněno, 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“ (body 88 a 89).
- 86 V tomto ohledu se „v čl. 15 odst. 1 první větě směrnice 2002/58 [...] stanoví, že účelem legislativních opatření, kterých se toto ustanovení týká a jež představují výjimku ze zásady důvěrnosti sdělení a souvisejících provozních údajů, musí být ‚zajištění národní bezpečnosti – tj. bezpečnosti státu – obrany, veřejné bezpečnosti nebo prevence, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému‘ nebo musí sledovat některý z jiných účelů stanovených v čl. 13 odst. 1 směrnice 95/46, na který odkazuje čl. 15 odst. 1 první věta směrnice 2002/58 (v tomto smyslu viz rozsudek ze dne 29. ledna 2008, Promusicae, C-275/06, EU:C:2008:54, bod 53). Povaha takového výčtu je taxativní, jak vyplývá z čl. 15 odst. 1 druhé věty směrnice 2002/58, podle jejíhož znění musí být legislativní opatření ospravedlněna ‚důvody uvedenými‘ v čl. 15 odst. 1 první větě uvedené směrnice. Z toho vyplývá, že členské státy taková opatření nemohou přijímat k jiným účelům, než které jsou uvedeny v posledně uvedeném ustanovení“ (bod 90).
- 87 Soudní dvůr dospěl ohledně rozsahu působnosti čl. 15 odst. 1 směrnice k tomuto závěru:
„Členské státy mohou přijímat opatření, která jsou výjimkou ze zásady důvěrnosti sdělení a s nimi souvisejících provozních údajů, pokud je toto opatření ‚v demokratické společnosti nezbytné, vhodné a přiměřené‘ s ohledem na účely, jež jsou uvedené v tomto ustanovení. Pokud jde o bod 11 odůvodnění této směrnice, je v něm upřesněno, že opatření této povahy musí být ‚plně‘ přiměřené vzhledem k zamýšlenému účelu. Stran uchovávání údajů je v čl. 15 odst. 1 druhé větě směrnice 2002/58 konkrétně upřesněn požadavek, podle kterého je uchovávání možné ‚po omezenou dobu‘ a ‚na základě důvodů‘ uvedených v čl. 15 odst. 1 první větě této směrnice“ (bod 95).
- 88 Soudní dvůr dále posoudil, zda taková vnitrostátní právní úprava, jako je úprava, která se vztahuje na první věc, která dala podnět k předběžným otázkám, jež mu byly předloženy, tyto podmínky splňuje. Konstatoval, že dotčená vnitrostátní právní úprava stanoví plošné a nerozlišující uchovávání veškerých provozních

a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahují na veškeré prostředky elektronické komunikace, a ukládá poskytovatelům služeb elektronických komunikací povinnost uchovávat tyto údaje systematicky a průběžně bez jakékoli výjimky. Takto uchovávané údaje umožňují dohledání a identifikaci zdroje sdělení a jeho adresáta, data, času a doby trvání komunikace, komunikačního vybavení uživatelů a zjištění polohy mobilního komunikačního zařízení (body 97 a 98).

- 89 Podle Soudního dvora lze z těchto údajů jako celku vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovány. Na základě těchto údajů lze tedy vytvořit profil dotčených osob, který je s ohledem na právo na ochranu soukromého života informací stejně citlivé povahy, jako je samotný obsah sdělení.
- 90 Předkládající soud v plném rozsahu cituje body 100 až 112 rozsudku Tele2 Sverige a Watson a další.
- 91 Soudní dvůr odpověděl na druhou předběžnou otázku ve věci C-203/15 a na první předběžnou otázku ve věci C-698/15 tak, že čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny musí být vykládán v tom smyslu, že brání vnitrostátní právní úpravě, která upravuje ochranu a bezpečnost provozních a lokalizačních údajů, zejména přístup příslušných vnitrostátních orgánů k uchovávaným údajům, a která v rámci boje proti trestné činnosti neomezuje tento přístup tak, aby byl umožněn výlučně pro účely boje proti závažné trestné činnosti, a nepodmiňuje tento přístup předchozím přezkumem ze strany soudu nebo nezávislého správního orgánu, a která nevyžaduje, aby dotčené údaje byly uchovávány na území Unie (bod 125).
- 92 Evropský soud pro lidská práva mezitím shledal, že švédské právní předpisy o masivním zachycování elektronických komunikací jsou v souladu s článkem 8 EÚLP (ESLP, 19. června 2018, Centrum för Rättvisa v. Švédsko, CE:ECHR:2018:0619JUD003525208). Jeho závěr o neexistenci porušení se zakládá na kritériích, která rozvedl ve své dřívější judikatuře (ESLP, 4. prosince 2015, Roman Zakharov v. Rusko, CE:ECHR:2015:1204JUD004714306). Uvedl zejména následující:
„Soud výslovně uznal, že vnitrostátní orgány mají široký prostor pro uvážení při výběru prostředků k zajištění národní bezpečnosti (cf. Weber a Saravia, § 106). Ve věcech Weber a Saravia a Liberty a další Soud připustil, že pravidla o masovém zachycování sama o sobě nepřekračují tento prostor. Vzhledem k argumentaci Soudu v těchto rozsudcích a k hrozbám, které v současné době existují v mnoha smluvních státech (zejména globální terorismus a jiné formy závažné trestné činnosti, jako je obchod s drogami, obchodování s lidmi, sexuální zneužívání dětí a kyberkriminalita), k technologickému vývoji, který teroristům a zločincům umožnil snadněji uniknout vysledování na internetu a k nepředvídatelnosti cest, kterými jsou elektronická sdělení přenášena, má Soud za to, že rozhodnutí využít systém masového zachycování za účelem identifikace dosud neznámých rizik pro národní bezpečnost je rozhodnutím, které vždy spadá

do prostoru pro uvážení členských států“ (ESLP, 19. června 2018, Centrum för Rättvisa v. Švédsko, CE:ECHR:2018:0619JUD003525208, § 112).

- 93 OBFG napadenému zákonu vytýká, že zachází stejným způsobem s uživateli telekomunikačních služeb či služeb elektronických komunikací, na které se vztahuje profesní tajemství, mimo jiné s advokáty, a s ostatními uživateli těchto služeb. Tato žalobkyně tvrdí, že zákon opět obsahuje plošnou povinnost zaznamenávat a uchovávat určitá metadata, která umožňují určit, zda se určitá fyzická nebo právnická osoba obrátila na advokáta, identifikovat tohoto advokáta, identifikovat osoby, které s ním mluvily a zejména jeho klienty, jakož i určit den a dobu komunikace. Tato plošná povinnost se vztahuje na všechny poskytovatele veřejně dostupných telefonních služeb pevné sítě, mobilních telefonních služeb, služeb přístupu k internetu, služeb internetové elektronické pošty, internetových telefonních služeb a veřejných elektronických komunikačních sítí.

Tatáž žalobkyně rovněž namítá, že napadený zákon stanoví plošnou povinnost uchovávat údaje, aniž rozlišuje mezi jednotlivci podle toho, zda jsou či nejsou předmětem vyšetřovacích úkonů nebo stíhání ohledně skutečností, které mohou vést k odsouzení v trestním řízení.

- 94 Dále tvrdí, že kategorie údajů, na které se zákon vztahuje, jsou mimořádně široké a rozmanité, neboť se vztahují na údaje sloužící k identifikaci uživatele nebo účastníka a komunikačních prostředků, údaje o přístupu a připojení koncového zařízení k síti a službě a o umístění tohoto zařízení, včetně koncového bodu sítě, jakož i komunikační údaje, přestože jejich obsah je naproti tomu vyloučen.
- 95 Neziskové sdružení Académie fiscale a jedna fyzická osoba napadenému zákonu vytýkají, že zachází stejným způsobem s uživateli telekomunikačních služeb či služeb elektronických komunikací, na které se vztahuje profesní tajemství, mimo jiné s účetními a daňovými poradci, a s ostatními uživateli těchto služeb, aniž je zohledněno zvláštní postavení účetních a daňových poradců, význam profesního tajemství, kterým jsou vázáni, a nezbytnost vztahu důvěry, který musí mít se svými klienty.
- 96 Napadenému zákonu rovněž vytýkají, že zachází stejným způsobem s jednotlivci, kteří jsou předmětem vyšetřovacích úkonů nebo stíhání ohledně skutečností, na které se vztahuje sporný účel uchovávání elektronických údajů, a s jednotlivci, kteří předmětem takových úkonů nejsou.
- 97 Nezisková sdružení Liga voor Mensenrechten a Ligue des Droits de l'Homme vytýkají napadenému zákonu, že stanoví plošnou povinnost uchovávat údaje, která ukládá provozovatelům a poskytovatelům veřejně dostupných telefonních služeb (a to i prostřednictvím internetu), služeb připojení k internetu, služeb internetové elektronické pošty a poskytovatelům veřejných elektronických komunikačních sítí, aby uchovávali po dobu dvanácti měsíců *de facto* ve vztahu ke všem Belgičanům, podezřelým či nikoliv, provozní údaje týkající se telefonních služeb pevné sítě, mobilních telefonních služeb a telefonních služeb

prostřednictvím internetu a údaje o připojení k internetu a aby tyto údaje poskytovali policii, soudním orgánům, zpravodajským a bezpečnostním službám, záchranným službám, Jednotce pro pohřešované osoby a Mediační službě pro telekomunikace.

- 98 Několik fyzických osob, které pobývají v Belgii a využívají různých služeb elektronických komunikací v rámci smlouvy uzavřené s provozovatelem, vytýkají napadenému zákonu, že stanoví plošnou a nerozlišující povinnost uchovávat identifikační údaje, údaje o připojení a lokalizační údaje a údaje o osobní komunikaci, která se ukládá poskytovatelům telefonních služeb, a to i prostřednictvím internetu, služeb připojení k internetu, služeb internetové elektronické pošty, provozovatelům veřejných elektronických komunikačních sítí, jakož i provozovatelům poskytujícím některou z těchto služeb.
- 99 Zákonomodárce zamýšlel stanovit tři kategorie metadat, které mají být uchovávány – identifikační údaje, údaje o přístupu a připojení a komunikační údaje –, zpřísnit podmínky přístupu k údajům ze strany příslušných orgánů a posílit zajištění údajů uchovávaných provozovateli, a to na základě výkladu rozsudků Soudního dvora, podle něhož je plošná povinnost uchovávat údaje přijatelná, pokud jsou spolu s ní přijaty takové záruky.
- 100 Článek 95 nařízení 2016/679 stanoví, že toto nařízení neukládá žádné další povinnosti fyzickým nebo právnickým osobám, pokud jde o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii, co se týče záležitostí, u nichž se na ně vztahují konkrétní povinnosti s tímž cílem stanovené ve směrnici 2002/58.
- 101 Článek 15 odst. 1 směrnice 2002/58 stanoví, že členské státy mohou mimo jiné přijmout legislativní opatření s cílem uchovávat údaje po určitou omezenou dobu z důvodů uvedených v tomto odstavci, mimo jiné pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, a to za podmínek stanovených v tomto ustanovení.
- 102 Napadený zákon mimo jiné stanoví podmínky, za kterých mohou zpravodajské a bezpečnostní služby získat údaje od poskytovatelů a provozovatelů.
- 103 V tomto ohledu je třeba uvést, že ve věci C-623/17 Privacy International položil soud členského státu Unie Soudnímu dvoru následující otázky:

„V případě, že:

a. možnosti [bezpečnostních a zpravodajských agentur (dále jen „BZA“) využívat [hromadné komunikační údaje (dále jen „HKÚ“), které jsou jim dodány, jsou nezbytné pro ochranu národní bezpečnosti Spojeného království, včetně oblastí boje proti terorismu, kontrašpionáže a boje proti šíření jaderných zbraní;

b. základním rysem využívání HKÚ ze strany BZA je odhalování dosud neznámých hrozeb pro národní bezpečnost prostřednictvím neadresných hromadných metod, které jsou závislé na shromažďování HKÚ na jednom místě. Jeho hlavní užitečnost spočívá v rychlé identifikaci a rozpracování cílů, jakož i v poskytnutí základny pro činnost v případě bezprostředního ohrožení;

c. poskytovatel sítě elektronických komunikací tudíž nemá povinnost uchovávat HKÚ (mimo dobu své obvyklé obchodní potřeby), které jsou tak uchovávány pouze státem (BZA);

d. vnitrostátní soud je názoru (s výhradou některých vyhrazených otázek), že záruky týkající se využívání HKÚ ze strany BZA jsou v souladu s požadavky EÚLP;

e. vnitrostátní soud je názoru, že při uplatnění podmínek stanovených v bodech 119 až 125 rozsudku [Tele2 Sverige a Watson a další] („podmínky Watson“) by byla zmařena opatření přijatá BZA za účelem ochrany národní bezpečnosti, čímž by došlo k ohrožení národní bezpečnosti Spojeného království;

1. Spadá požadavek v pokynu ministra adresovaný poskytovateli sítě elektronických komunikací, aby poskytoval hromadné komunikační údaje bezpečnostním a zpravodajským agenturám („BZA“) členského státu, s ohledem na článek 4 SEU a čl. 1 odst. 3 směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „směrnice o soukromí a elektronických komunikacích“), do oblasti působnosti unijního práva a směrnice o soukromí a elektronických komunikacích?

2. V případě kladné odpovědi na první otázku, bude se na takový pokyn ministra vztahovat jakákoliv z podmínek Watson nebo jakákoli jiná podmínka nad rámec těch stanovených v EÚLP? A pokud ano, jak a v jakém rozsahu se tyto podmínky uplatní, vzhledem k nezbytnosti využívání metod hromadného shromažďování a automatického zpracovávání ze strany BZA za účelem ochrany národní bezpečnosti a vzhledem k rozsahu, ve kterém tyto možnosti, jež jsou jinak v souladu s EÚLP, mohou být uplatněním takových podmínek kriticky oslabeny?“

104 Předkládající soud bude muset při svém přezkumu zohlednit odpověď na tyto předběžné otázky.

105 Napadený zákon rovněž stanoví podmínky, za kterých mohou soudní orgány získat údaje za účelem vyhledávání, vyšetřování a stíhání trestných činů.

106 Je proto třeba rovněž vyčkat odpovědi Soudního dvora na předběžnou otázku, která mu byla položena ve věci C-207/16 Ministerio Fiscal:

„Lze dostatečnou závažnost trestných činů jako kritérium, které odůvodňuje zásah do základních práv zakotvených v člancích 7 a 8 Listiny, určit výlučně s ohledem na trest, který lze za vyšetřovaný trestný čin uložit, nebo je navíc nezbytné v trestném jednání identifikovat zvláštní míru poškození individuálních nebo

kolektivních právních zájmů?

Jaký by měl být minimální práh trestu, pokud určení závažnosti trestného činu pouze s ohledem na trest, který lze uložit, případně vyhovuje unijním ústavním zásadám uplatněným Soudním dvorem Evropské unie v rozsudku [Digital Rights] jako standardům pro přísný přezkum směrnice [která byla uvedeným rozsudkem zrušena]? Byl by vyhovující obecný minimální práh odpovídající sazbě tří let odnětí svobody?“

Ze stanoviska generálního advokáta Saugmandsgaarda Øe v této věci (C-207/16, EU:C:2018:300) vyplývá, že relevantní ustanovení mohou být vykládána několika způsoby.

- 107 Ve zbývající části se účastníci řízení před předkládajícím soudem neshodují ohledně výkladu několika ustanovení, zejména čl. 15 odst. 1 směrnice 2002/58 a článků 7, 8, 11 a 52 Listiny, které musí předkládající soud učinit součástí přezkumu napadeného zákona.
- 108 Jak uvádějí žalobci, Soudní dvůr však v rozsudku Tele2 Sverige a Watson a další rozhodl, že čl. 5 odst. 1 směrnice 2002/58 stanoví základní povinnost, podle které musí být zajištěna důvěrnost sdělení a s nimi souvisejících provozních údajů, a čl. 15 odst. 1 téže směrnice, obsahující výjimky z této zásady, musí být vykládán restriktivně, aby bylo zabráněno tomu, že se výjimka ze zásady stanovené v článku 5 směrnice stane pravidlem, neboť jinak by bylo toto posledně uvedené ustanovení zbaveno jeho působnosti.
- 109 Soudní dvůr rovněž zdůraznil, že opatření, která jsou výjimkou ze zásady důvěrnosti sdělení a s nimi souvisejících provozních údajů, mohou být odůvodněna pouze s ohledem na účely uvedené v článku 15, přičemž článek 15 v tomto ohledu stanoví požadavek, podle kterého je uchovávání údajů možné pouze po omezenou dobu a na základě uvedených důvodů.
- 110 Jak proto zdůrazňují žalobci, Soudní dvůr má za to, že vnitrostátní právní úprava, která ukládá plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace, a to bez vyrozumění uživatelů, představuje zvláště závažný zásah do základních práv zakotvených v článcích 7 a 8 Listiny, takže takové opatření může být odůvodněno pouze bojem proti závažné trestné činnosti. Soudní dvůr dodává, že i když se jedná o cíl obecného zájmu, nemůže sám o sobě odůvodnit, že vnitrostátní právní úprava, která stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů, je považována za nezbytnou pro účely uvedeného boje.
- 111 Soudní dvůr z toho vyvodil, že vnitrostátní právní úprava, která nestanovuje žádné rozlišení, omezení nebo výjimky v závislosti na sledovaném cíli, která se týká globálně všech osob, které využívají služeb elektronických komunikací, bez zeměpisného nebo časového rozlišení, aniž se zohledňuje skutečnost, že se tyto

osoby nachází byt' nepřímo v situaci, která může vést k trestnímu stíhání, nebo že se komunikace údajů týká osob, jejichž sdělení jsou předmětem profesního tajemství, a aniž se vyžaduje souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti, překračuje meze toho, co je naprosto nezbytné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje článek 15 směrnice ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny.

- 112 Podle žalobců je sice pravda, že Soudní dvůr uvádí, že čl. 15 odst. 1 směrnice 2002/58 nebrání vnitrostátní právní úpravě, která umožňuje cílené uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti za podmínky, že uchovávání je omezeno na to, co je nezbytně nutné, pokud jde o kategorie údajů, které mají být uchovávány, komunikační prostředky, na něž se toto uchovávání vztahuje, dotčené osoby a dobu trvání uchovávání. To znamená, že vnitrostátní právní úprava musí stanovit jasná a přesná pravidla a zajistit, aby osoby, kterých se týká uchovávání údajů, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití. Soudní dvůr dodává, že vnitrostátní právní úprava musí zejména vymezit okolnosti a podmínky, za nichž může být preventivně přijato opatření pro uchovávání údajů. Taková právní úprava musí být založena na objektivních skutečnostech, na jejichž základě lze vymezit okruh osob z řad veřejnosti, jejichž údaje mohou vykazat souvislost se závažnou trestnou činností nebo které představují závažné ohrožení veřejné bezpečnosti, přičemž toto vymezení lze zajistit prostřednictvím zeměpisného kritéria, jestliže příslušné vnitrostátní orgány mají na základě objektivních skutečností za to, že v jedné nebo více z územních oblastí existuje zvýšené riziko přípravy či páchaní takových trestných činů.
- 113 Zákonodárce přitom přijetím napadeného zákona sleduje širší cíle, než je boj proti závažné trestné činnosti či závažnému ohrožení veřejné bezpečnosti.
- 114 Zákonodárce rovněž několikrát v rámci přípravných prací uvedl, že pokud jde o samotnou zásadu spočívající v povinnosti uchovávat údaje, zamýšlel ji vztáhnout na všechny osoby, i když dosud nejsou předmětem vyšetřování; nestanovil ostatně žádná rozlišení v závislosti na časovém období, zeměpisné oblasti nebo okruhu osob a nestanovil ani výjimku ve vztahu k osobám, na jejichž sdělení se vztahuje profesní tajemství.
- 115 Žalobci tvrdí, že i když byly podmínky přístupu k uchovávaným údajům v napadeném zákoně podstatně zpřísněny, plošná povinnost uchovávání údajů, kterou stanoví, nesplňuje podle výkladu Soudního dvora v rozsudku Tele2 Sverige a Watson a další požadavky stanovené v čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny. Taková povinnost totiž překračuje meze toho, co je naprosto nezbytné, a nelze ji považovat za odůvodněnou v demokratické společnosti, jak to vyžadují výše uvedená ustanovení unijního práva.
- 116 Rada ministrů zdůrazňuje, že napadená právní úprava sleduje několik cílů. Zákonodárce nejprve usiluje o zlepšení dlouhotrvající situace, v níž je v rámci

trestního vyšetřování získáván přístup k údajům v odvětví telekomunikací, a to vytvořením legislativního rámce poskytujícího nezbytné záruky v oblasti ochrany soukromí. Povinnost uchovávat údaje je rovněž uložena za účelem zjišťování pravdy ohledně čtených forem trestné činnosti, a tím směřuje k zajištění integrity systému trestního soudnictví. Toto zjišťování pravdy je v zájmu jak oběti i obžalovaného (který může například prokázat, že se v rozhodné době nacházel na jiném místě), tak všech ostatních dotčených osob. Povinnost uchovávat údaje je rovněž vyžadována za účelem zásahu v návaznosti na tísňové volání či pátrání po pohřešované osobě, jejíž tělesná integrita je bezprostředně ohrožena. Tato skutečnost představuje podstatný rozdíl ve srovnání se situacemi, které byly uvedeny ve výše uvedených rozsudcích Soudního dvora. Existuje tedy vztah proporcionality mezi plošnou povinností uchovat údaje a cílem, který si zákonodárce stanovil.

- 117 Rada ministrů dále zdůrazňuje, že zákonodárce neměl za to, že je s ohledem na sledovaný cíl možné zavést cílenou a rozlišující povinnost uchovávat údaje a že se rozhodl spojit plošnou a nerozlišující povinnost uchovávat údaje se striktními zárukami, a to jak z hlediska ochrany uchovávání, tak z hlediska přístupu, aby byl co nejvíce omezen zásah do práva na ochranu soukromého života. V tomto ohledu Rada ministrů zdůrazňuje, že je jednoduše nemožné předem rozlišovat z hlediska osob, časových období a zeměpisných oblastí. Odkazuje v tomto ohledu rovněž na stanovisko generálního advokáta Saugmandsgaarda Øe ve spojených věcech C-203/15 a C-698/15, *Tele2 Sverige a další*, EU:C:2016:572.
- 118 Z informací, které má k dispozici předkládající soud, vyplývá, že většina členských států se ostatně potýká se značnými obtížemi při zajištění souladu svých právních předpisů v oblasti uchovávání údajů s požadavky, které stanovil Soudní dvůr ve své judikatuře (viz *Data retention across the EU*, <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>; dopis ministra spravedlnosti a bezpečnosti Nizozemska ze dne 26. března 2018 předsedovi „Tweede Kamer der Staten-Generaal“, druhý senát, období 2017–2018, 34 537, č. 7).
- 119 Je proto třeba položit Soudnímu dvoru první předběžnou otázku uvedenou ve výroku.
- 120 Cílem napadeného zákona je rovněž umožnit účinné vedení trestního vyšetřování a stanovit účinné sankce za sexuální zneužívání mladistvých a umožnit skutečnou identifikaci pachatele takového trestného činu, i když jsou používány prostředky elektronické komunikace. Na jednání bylo v tomto ohledu upozorněno na pozitivní povinnosti, které vyplývají z článků 3 a 8 EÚLP ohledně ochrany tělesné a duševní integrity mladistvých a jiných zranitelných osob, jak jsou vykládány EÚLP (EÚLP, 2. prosinec 2008, K.U. v. Finsko, CE:ECHR:2008:1202JUD000287202, §§46 až 49). Tyto povinnosti by mohly také vyplývat z odpovídajících ustanovení Listiny, což by mohlo mít důsledky pro výklad čl. 15 odst. 1 směrnice 2002/58.

121 Je proto třeba položit druhou předběžnou otázku uvedenou ve výroku.

122 Konečně je třeba položit třetí předběžnou otázku uvedenou ve výroku.

VIII. Předběžné otázky

123 Ústavní soud předkládá Soudnímu dvoru Evropské unie 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 a právem na ochranu osobních údajů, jak je zaručeno články 7, 8 a čl. 52 odst. 1 Listiny základních práv Evropské unie, 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 (EU) 2016/679, a která kromě toho podléhá zárukám stanoveným v této právní úpravě ohledně uchovávání údajů a přístupu k nim?

2. Musí být čl. 15 odst. 1 směrnice 2002/58/ES ve spojení s články 4, 7, 11 a čl. 52 odst. 1 Listiny základních práv Evropské unie 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 Ústavní soud na základě odpovědí poskytnutých na první a druhou předběžnou otázku dospět k závěru, že napadený zákon porušuje jednu či více povinností vyplývajících z ustanovení uvedených v těchto otázkách, mohl by dočasně zachovat účinky zákona ze dne 29. května 2016 o shromažďování a uchovávání údajů v odvětví elektronických komunikací s cílem vyhnout se právní nejistotě a zajistit, aby mohly být předtím shromážděné a uchované údaje dále využívány pro účely stanovené zákonem?