Česká republika
NÁLEZ
Ústavního soudu

Jménem republiky

Plénum Ústavního soudu ve složení Stanislav Balík, František Duchoň, Vlasta Formánková, Vojen Güttler, Pavel Holländer, Vladimír Kůrka, Dagmar Lastovecká, Jan Musil, Jiří Nykodým, Pavel Rychetský, Miloslav Výborný a Eliška Wagnerová (soudce zpravodaj) rozhodlo dne 22. března 2011 o návrhu **skupiny poslanců Poslanecké sněmovny Parlamentu České republiky**, zastoupené poslancem Markem Bendou, se sídlem Praha 1, Sněmovní 4, na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, za účasti Poslanecké sněmovny a Senátu Parlamentu České republiky jako účastníků řízení,

t a k t o :

Ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, se r u š í dnem vyhlášení tohoto nálezu ve Sbírce zákonů.

O d ů v o d n ě n í:

I.
Rekapitulace návrhu

1.Skupina 51 poslanců Poslanecké sněmovny Parlamentu České republiky se návrhem doručeným Ústavnímu soudu dne 26. 3. 2010 domáhala zrušení ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále též jen „napadená ustanovení“), a vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání (dále též jen „napadená vyhláška“ či souhrnně též jen „napadená právní úprava“).

2.Byť návrh splňoval formální náležitosti dle čl. 87 odst. 1 písm. a) Ústavy České republiky a § 64 odst. 1 písm. b) zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů (dále jen „zákon o Ústavním soudu“), považuje Ústavní soud za nezbytné zdůraznit, že institut návrhu na zrušení zákona nebo jeho jednotlivých ustanovení dle čl. 87 odst. 1 písm. a) Ústavy České republiky, podávaný skupinou poslanců či senátorů dle § 64 odst. 1 písm. b) zákona o Ústavním soudu, je mimo jiné projevem ústavně garantovaného principu ochrany menšin (čl. 6 Ústavy České republiky) a primárně slouží jako jeden z nástrojů ochrany parlamentní menšiny (opozice) proti případné svévoli (či zvůli) v rozhodnutích přijímaných parlamentní většinou v rámci legislativního procesu,

založeného na principu většinového rozhodování [srov. k tomu zprávu Benátské komise CDL-AD(2010)025 „*Report on the role of the opposition in a democratic parliament*“ ze dne 15. 11. 2010, která právo umožňující parlamentní opozici domáhat se ústavního přezkumu většinou přijatých rozhodnutí (zákonů) zahrnuje mezi nejzákladnější práva parlamentní opozice]. Jinými slovy, kvalifikované podání k nestrannému a nezávislému Ústavnímu soudu je často poslední možností, jak se parlamentní menšina může případné svévoli (či zvůli) v rozhodování parlamentní většiny bránit, neboť zástupci parlamentní opozice se v Parlamentu co do svého počtu zpravidla ocitají v početní menšině a nedisponují tak efektivními prostředky, jak přijetí takového rozhodnutí (vydání normativního právního aktu) v rámci legislativního procesu zvrátit či změnit. Naopak zástupci parlamentní většiny takovými efektivními prostředky zpravidla disponují a mají-li pochybnosti o správnosti, bezvadnosti či dokonce o ústavnosti přijímaných (či dříve přijatých) rozhodnutí, je nejen jejich právem, ale přímo i povinností je za tímto účelem využívat (viz slib dle čl. 23 odst. 3 Ústavy České republiky). Institut podání návrhu na zrušení zákona nebo jeho jednotlivých ustanovení dle čl. 87 odst. 1 písm. a) Ústavy České republiky k Ústavnímu soudu tak v žádném případě neslouží jako prostředek, jak získat jakési „dobrozdání“ či odborný posudek Ústavního soudu k parlamentní většinou přijatým rozhodnutím, ani jako nástroj, jehož uplatnění je projevem politického či dokonce předvolebního boje přeneseného z parlamentní půdy k Ústavnímu soudu. V posuzovaném případě nejen že skupina navrhovatelů je složena zejména ze zástupců politických stran, jež se v současnosti podílejí a rovněž v době podání návrhu se podílely na výkonu vládní moci a v Parlamentu České republiky disponovaly a dále disponují většinou potřebnou ke změně napadené právní úpravy, ale navíc, a to nemůže Ústavní soud ponechat bez kritické poznámky, se z drtivé většiny svým souhlasným (!) hlasováním v průběhu legislativního procesu na přijetí napadené právní úpravy přímo podíleli. V takových případech jeho (zne)užití by Ústavní soud byl do budoucna nucen přistoupit k odmítání takto podaných návrhů.

3.Podstatu námitek navrhovatelé sami shrnuli tak, že shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu v takovém rozsahu, v jakém jej vymezují napadená ustanovení a napadená vyhláška, představují neproporcionální zásah do základních práv uvedených v Listině základních práv a svobod (dále jen „Listina“) a v Úmluvě o ochraně lidských práv a základních svobod (dále jen „Úmluva“), konkrétně základních práv garantovaných čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 Listiny a čl. 8 Úmluvy. Dle navrhovatelů lze tento zásah navíc považovat za porušující podstatné náležitosti demokratického právního státu, k nimž lze přiřadit i zásadu proporcionality ve smyslu čl. 4 odst. 4 Listiny. Svá tvrzení navrhovatelé podepřeli následujícími argumenty.

I. A) Shromažďování údajů o komunikaci jako zásah do soukromého života

4.Obsahem napadaných ustanovení je uložení povinnosti fyzickým a právnickým osobám, které zajišťují veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací (tedy především telefonních operátorů a poskytovatelů internetového připojení), po dobu 6 až 12 měsíců uchovávat provozní a lokalizační údaje (desítky údajů) o veškeré telefonní a faxové komunikaci, e-mailové a SMS komunikaci, návštěvách webových stránek a využívání některých internetových služeb, specifikované v napadené vyhlášce, a na žádost jsou povinny je poskytovat oprávněným orgánům. Dle navrhovatelů výše uvedené údaje, jejich shromažďování, uchovávání a předávání státním orgánům nepochybně spadají pod ochranu čl. 8 Úmluvy. V této souvislosti odkázali na celou řadu rozhodnutí Evropského soudu pro lidská práva (dále jen „ESLP“) i Ústavního soudu.

5.Navrhovatelé jsou dále toho názoru, že zásahem do základních práv se nerozumí jen

bezprostřední zásah (např. seznámení se s uchovávanými údaji), ale i taková opatření státních orgánů, která v sobě skrývají značné nebezpečí omezení základních práv, které může kdykoliv nastat. Uchovávání provozních a lokalizačních údajů nelze než považovat za takový zásah, neboť tyto údaje jsou nepřetržitě uchovávány a státním orgánům jsou k dispozici a mohou si je v budoucnu dle příslušných předpisů vyžádat a využívat. Uchovávání shora uvedené sady údajů tak s sebou nese latentní nebezpečí dalších bezprostředních zásahů státních orgánů. Navíc nelze přehlédnout, že stát neuchovává provozní a lokalizační údaje sám, ale využívá k tomu soukromých osob poskytujících telekomunikační služby, přičemž riziko z možného zneužití uchovávaných údajů velkým počtem soukromých osob pohybujících se v oblasti telekomunikačních služeb je vyšší než při jejich uchovávání státem. Jedním ze základních požadavků ESLP, vyvinutých výkladem podmínky zákonného podkladu státních zásahů do soukromého života, je předvídatelnost a dostupnost tohoto zákonného podkladu. Důvodem je legitimní a logický požadavek, aby jednotlivci byli předem seznámeni s okolnostmi, kdy stát může výjimečně do jejich soukromého života zasáhnout, a mohli přizpůsobit své jednání tak, aby se tomuto zásahu bylo možné vyhnout. Plošný charakter uchovávání provozních a lokalizačních údajů však takovou možnost omezuje až vylučuje.

6.Dle navrhovatelů jsou cíle, jakož i pravděpodobný a očekávatelný užitek vyplývající z povinnosti uchovávat provozní a lokalizační údaje, ve srovnání s tím spojeným zásahem do základních práv dotčených osob, v hrubém nepoměru. Proto v souladu s čl. 8 odst. 2 Úmluvy přistoupili k posouzení přiměřenosti daného opatření, které hodnotili jednak z hlediska závažnosti a rozsahu zásahu do základních práv jednotlivců, v daném případě do práva na soukromí, dále z hlediska legitimity cíle, k jehož dosažení má omezení základních práv sloužit, a z hlediska přínosu těchto zásahů. V neposlední řadě jeho užití konfrontovali s nebezpečnými aspekty, které jsou s tím spojeny, zejména pak nebezpečí zneužití uchovávaných údajů.

I. B) Závažnost a rozsah zásahu do práva na soukromí

7.Předně navrhovatelé konstatovali, že zavedení povinnosti uchovávat provozní a lokalizační údaje představuje závažný zásah do soukromí, poněvadž tyto údaje otevírají široké možnosti jejich použití a jejich zkombinování s dalšími údaji může způsobit velmi citelné důsledky pro soukromý život dotčených osob. Povinnost uchovávat provozní a lokalizační údaje v takovém rozsahu má prakticky za následek vyloučení existence nekontrolované a nemonitorované telekomunikace, což je nutno považovat za obzvlášť intenzivní zásah do soukromí všech osob užívajících telekomunikační prostředky (telefonie, užívání služeb internetu), které se v současnosti již nevyužívají pouze ke komunikaci mezi lidmi, ale zasahují široké spektrum každodenních činností (nakupování, bankovní operace, vzdělávání, medicína aj.). Z uchovávaných údajů tak lze dovodit celou řadu dalších (v řadě případů velmi citlivých) údajů a informací o dané osobě a jejím soukromí. V řadě případů lze z identity adresáta telefonátu nebo e-mailu odhalit citlivý údaj o odesílateli (např. pokud je adresátem lékař-specialista), podobně lze z navštívených internetových stránek zjišťovat informace o názorovém smýšlení, zdravotním stavu nebo sexuální orientaci dané osoby. Velké množství informací lze získat rovněž z lokalizačních údajů o pohybu mobilního telefonu (respektive jeho držitele), zvláště v kombinaci s lokalizačními údaji o pohybu dalších mobilních telefonů (údaj o tom, kdo se kde a kdy s kým setkal apod.). Na základě uchovávaných údajů tak lze sestavit komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti, což rovněž představuje významný zásah do práva na ochranu soukromí a korespondence jednotlivců.

I. C) Legitimita cíle a přínos zásahu do základních práv

8.Navrhovatelé dále ve svém návrhu polemizovali s legitimitou cíle přijetí napadené úpravy. Z důvodové zprávy vlády k ustanovení § 97 zákona o elektronických komunikacích vyplývá, že účelem ust. § 97 je čelit zvyšujícím se bezpečnostním rizikům a zajištění bezpečnosti a obrany České republiky, přičemž bližší odůvodnění chybí. Navrhovatelé jsou toho názoru, že podle čl. 8 odst. 2 Úmluvy je zásah do soukromí přípustný ve vztahu k boji s kriminalitou pouze tehdy, pokud slouží k předcházení zločinnosti. „*Preventivní, všeobecné uchovávání telekomunikačních údajů bez existence konkrétního důvodu míří zejména do minulosti a může tak sloužit hlavně k objasňování již spáchaných trestných činů*." (str. 13). Zásah do soukromí za účelem objasnění již spáchaného trestného činu je tak dle navrhovatelů v rozporu s čl. 8 Úmluvy. Navíc údaje jsou uchovávány bez existence konkrétního podezření. Optikou napadených ustanovení je tak každá osoba považována za podezřelou bez existence konkrétních okolností, které by k tomuto podezření opravňovaly, což je v právním státě nepřípustné. Navrhovatelé rovněž upozornili (s odkazem na konkrétní případy ze zahraničí) na skutečnost, že vyhodnocování údajů o telekomunikačním provozu s sebou přináší rovněž nebezpečí jejich chybné interpretace a podezřívání či obvinění nevinného člověka. Může totiž dojít k záměně osoby, která komunikaci skutečně prováděla s osobou, která např. uzavřela smlouvu s telefonním operátorem nebo s poskytovatelem internetu.

9.Předkladatelé právní úpravy ani věcně příslušný resort státní správy dle tvrzení navrhovatelů nedodali informace o tom, v kolika a v jakých případech před zavedením napadené právní úpravy, která s sebou nese obrovské kvantitativní navýšení uchovávaných údajů a možného přístupu k nim, ztroskotávalo vyšetřování, odhalování a stíhání závažných trestných činů, na nemožnosti získat požadované údaje z důvodu, že již taková data nebyla k dispozici. Rovněž není prokázané, zda zakotvení povinnosti uchovávat všechny údaje o telefonické a elektronické komunikaci povede (nebo již vedlo) ve srovnání s předcházející úpravou skutečně ke zlepšení vyšetřování, k odhalování a ke stíhání závažných trestných činů a k odvracení hrozeb, ke zvýšení procenta objasněnosti trestných činů či ke snížení kriminality apod. Dále je otázkou, jak stará data jsou oprávněnými orgány vyžadována a nakolik je tedy nutné uchovávat provozní a lokalizační údaje po dobu 6 měsíců a delší. Zásah do soukromí se navíc paradoxně může častěji týkat osob, které se na závažné trestné činnosti nepodílejí, než osob, které ji páchají, a proto mají zvýšený zájem na uskutečňování anonymní komunikace. Dle navrhovatelů lze očekávat, že uchovávání údajů může pomoci k naplnění stanovených cílů spíše v malé míře a v méně významných případech, a proto nelze očekávat dlouhodobý a pozitivní vliv na snížení kriminality a zvýšení bezpečnosti v souvislosti s používáním telekomunikačních prostředků.

I. D) Nebezpečí zneužití uchovávaných údajů

10. Stejně tak je dle navrhovatelů třeba počítat i s rizikem nezákonného použití a zneužití uchovávaných údajů, neboť při tak velkém množství společností, které zajišťují telekomunikaci (zejména v případě mobilní komunikace a internetu), nelze očekávat odpovídající zajištění těchto provozních a lokalizačních údajů. Proto je nutno zkoumat i reálné a technicky existující možnosti jejich použití. Napadená právní úprava dle navrhovatelů nestanoví ani podmínky, na jejichž základě mají být údaje uchovávány, ani podmínky pro jejich užití oprávněnými orgány, jakož ani negarantuje jednotlivcům žádné záruky proti jejich zneužití. Napadená právní úprava tak nahrává extenzivnímu využívání příslušných databází, jak co do množství údajů, které z nich budou čerpány, tak i množství subjektů, které k tomuto budou oprávněny, a rovněž umožňuje rozšiřování účelů, k nimž

budou údaje využívány. Velmi reálné je dle navrhovatelů rovněž nebezpečí zneužití provozních a lokalizačních údajů ze strany třetích osob. Osobami, které mohou tyto osobní údaje zneužít, jsou velmi často zaměstnanci společností nebo státních orgánů, které údaje zpracovávají, tak i další osoby (např. tzv. hackeři).

I. E) Předběžná otázka k Evropskému soudnímu dvoru

11. V závěru svého návrhu vyjádřili navrhovatelé přesvědčení, že byť je napadená právní úprava úpravou vnitrostátní, na kterou je třeba vztáhnout kritéria vyplývající z ústavního pořádku České republiky, jedná se současně o problematiku, jejíž původ pramení z komunitárního práva, konkrétně z transpozice směrnice Evropského parlamentu a Rady č. 2006/24/ES (dále též jen „Směrnice o data retention“) do právního řádu České republiky. Ze stejných, výše rozvedených důvodů proto navrhovatelé předestřeli Ústavnímu soudu ke zvážení možnost předložit Evropskému soudnímu dvoru v souladu s čl. 234 Smlouvy o ES předběžnou otázku týkající se (ne)platnosti samotné Směrnice o data retention, neboť existuje významné riziko, že dotčená Směrnice, jež byla napadenými ustanoveními a napadenou vyhláškou transponována do českého právního řádu, je v rozporu s právem ES.

II.
Rekapitulace vyjádření účastníků řízení

12. Ústavní soud podle ustanovení § 42 odst. 4 a § 69 zákona o Ústavním soudu zaslal předmětný návrh na zrušení napadených ustanovení a napadené vyhlášky Poslanecké sněmovně a Senátu Parlamentu České republiky a rovněž veřejnému ochránci práv.

13. Poslanecká sněmovna Parlamentu České republiky, zastoupená předsedou Ing. M. Vlčkem, ve svém vyjádření ze dne 26. 4. 2010 podrobně popsala proceduru přijetí vládního návrhu zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, na jehož základě se napadená ustanovení stala součástí zákona č. 127/2005 Sb., o elektronických komunikacích (blíže viz část IV. nálezu). K obsahu vládního návrhu zákona nadto konstatovala, že v důvodové zprávě vláda výslovně uvedla, že předkládaný návrh zákona je v souladu s ústavním pořádkem a právním řádem České republiky a neodporuje mezinárodním smlouvám, jimiž je Česká republika vázána. Ze stejného přesvědčení vycházela při jeho projednávání i Poslanecká sněmovna. Je tak na Ústavním soudu, aby posoudil ústavnost napadených ustanovení.

14. Senát Parlamentu České republiky, zastoupený předsedou MUDr. P. Sobotkou, ve svém vyjádření ze dne 28. 4. 2010 poté, co obsáhle rekapituloval argumentaci navrhovatelů obsaženou v posuzovaném návrhu, rovněž popsal proceduru přijímání předmětného vládního návrhu zákona Senátem (blíže viz část IV. nálezu). K průběhu jeho projednávání dále uvedl, že jak ve Výboru pro hospodářství, zemědělství a dopravu, tak ve Stálé komisi Senátu pro sdělovací prostředky a později i na plénu Senátu byl návrh zákona představen jako další novela reagující na povinnost České republiky transponovat příslušnou směrnici ES do našeho právního řádu. K povinnosti telekomunikačních operátorů, internetových providerů a dalších, kteří působí na úseku elektronických komunikací, uchovávat, po dobu nejméně 6 měsíců lokalizační a provozní údaje, bylo předkladatelem zdůrazněno, že „*v žádném případě se nejedná o něco, co by se dalo přirovnat k odposlechům, už jen proto, že se neuchovávají obsahy jednotlivých telefonátů nebo mailových zpráv, a protože jde i o služby internetu* (...), *uchovávají se pouze lokalizační a provozní údaje, tedy technická data*". Senát tuto skutečnost při projednávání návrhu předmětné novely zákona

akceptoval a na základě doporučení výboru i Stálé komise Senátu pro sdělovací prostředky, návrh zákona schválil ve znění přijatém Poslaneckou sněmovnou. Je proto jen na Ústavním soudu, aby návrh na zrušení předmětných ustanovení zákona o elektronických komunikacích posoudil a s konečnou platností rozhodl.

15. Veřejný ochránce práv JUDr. Otakar Motejl svým vyjádřením ze dne 12. 4. 2010 sdělil, že po prostudování zaslaného návrhu se s předkládanými argumenty neztotožňuje, a proto nevstupuje do řízení o zrušení napadené vyhlášky před Ústavním soudem.

III.
Upuštění od ústního jednání

16. Podle ustanovení § 44 odst. 2 zákona o Ústavním soudu může Ústavní soud se souhlasem účastníků upustit od ústního jednání, nelze-li od tohoto jednání očekávat další objasnění věci. Ústavní soud si proto v souladu s tímto ustanovením vyžádal od účastníků řízení vyjádření, zda souhlasí s upuštěním od ústního jednání. Navrhovatelé i Senát Parlamentu České republiky souhlas vyslovili, Poslanecká sněmovna Parlamentu České republiky na výzvu ve lhůtě jí určené nijak nereagovala. Od ústního jednání tak mohlo být v posuzované věci upuštěno.

IV.
Ústavní konformita procedury přijímání napadených ustanovení zákona a zákonné podmínky přijetí napadené vyhlášky

17. Při řízení o kontrole norem dle čl. 87 odst. 1 písm. a) Ústavy České republiky ve smyslu ust. § 68 odst. 2 zákona o Ústavním soudu, musí Ústavní soud nejprve zkoumat, zda byl předmětný zákon přijat a vydán ústavně předepsaným způsobem [k algoritmu přezkumu v řízení o kontrole norem viz bod. 61 nálezu sp. zn. Pl. ÚS 77/06 ze dne 15. 2. 2007 (N 30/44 SbNU 349; 37/2007 Sb.)]. V případě podzákonných právních předpisů, konkrétně vyhlášek ministerstev, Ústavní soud podle § 68 odst. 2 zákona o Ústavním soudu posuzuje, zda byly přijaty a vydány v mezích Ústavou České republiky stanoveného oprávnění (čl. 79 odst. 3 Ústavy České republiky), tj. zda nebyly vydány *„ultra vires“*.

18. Z vyjádření obou komor Parlamentu České republiky, připojených příloh a dokumentů dostupných elektronickou cestou (usnesení a tisky dostupné v digitální knihovně na webových stránkách Poslanecké sněmovny a Senátu, na www.psp.cz a www.senat.cz) Ústavní soud zjistil následující: Napadená ustanovení § 97 odst. 3 a 4 se stala součástí zákona č. 127/2005 Sb., o elektronických komunikacích, na základě zákona č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Návrh tohoto zákona předložila Poslanecké sněmovně vláda České republiky dne 16. 1. 2008, přičemž navrhla jeho projednávání tak, aby s ním Poslanecká sněmovna mohla vyslovit souhlas již v 1. čtení. Poslancům byl návrh rozeslán dne 18. 1. 2008 jako sněmovní tisk č. 398/0 – *Novela zákona o elektronických komunikacích - EU*. V 1. čtení, které proběhlo dne 30. 1. 2008 na 27. schůzi, Poslanecká sněmovna nesouhlasila s projednáváním tak, aby mohla s návrhem zákona vyslovit souhlas již v prvém čtení. Návrh zákona byl následně přikázán k projednání Hospodářskému výboru, Ústavně právnímu výboru a Výboru pro bezpečnost (usnesení č. 593). Příslušné výbory jej projednaly a jejich usnesení s pozměňovacími návrhy byla poslancům doručena jako tisky č. 398/1, 398/2 a 398/3. Pouze pozměňovací návrhy Výboru pro bezpečnost se týkaly i napadeného

ust. § 97 odst. 3 (třetí a páté věty). Na 28. schůzi Poslanecké sněmovny se ve dnech 20. 3. 2008 a 25. 3. 2008 konalo 2. čtení, návrh zákona prošel obecnou a podrobnou rozpravou, v jejímž průběhu byly k napadeným ustanovením (§ 97 odst. 3 třetí a pátá věta a § 97 odst. 4) podány pozměňovací návrhy i ze strany jednotlivých poslanců (pozměňovací návrhy Z. Bebarové-Rujbrové, K. Jacques a J. Klase). Podané pozměňovací návrhy byly zpracovány jako tisk 398/4, který byl poslancům rozeslán dne 25. 3. 2008. 3. čtení proběhlo dne 23. 4. 2008 na 30. schůzi Poslanecké sněmovny. Navrhované pozměňovací návrhy k napadeným ustanovením § 97 odst. 3 a 4 přijaty nebyly. Návrh zákona byl ve znění dalších schválených pozměňovacích návrhů přijat (usnesení č. 736) poté, co s ním Poslanecká sněmovna vyslovila souhlas, kdy z přítomných 176 poslanců a poslankyň pro návrh hlasovalo 89, proti 21, zdrželo se 66 (hlasování č. 44).

19. Předmětný návrh zákona byl Senátu Poslaneckou sněmovnou postoupen dne 19. 5. 2008. Organizační výbor Senátu jej jako senátní tisk č. 247 určil k projednání Výboru pro hospodářství, zemědělství a dopravu. Kromě toho návrh zákona projednala i Stálá komise Senátu pro sdělovací prostředky. Výbor na svém zasedání dne 28. 5. 2008 přijal usnesení č. 270, ve kterém doporučil Senátu návrh zákona schválit. Rovněž Stálá komise Senátu pro sdělovací prostředky doporučila Senátu návrh zákona schválit (usnesení č. 22 ze dne 4. 6. 2008). Senát návrh zákona projednal dne 5. 6. 2008 na své 14. schůzi (6. funkční období) a přijal k návrhu usnesení č. 402, kterým schválil návrh zákona ve znění postoupeném mu Poslaneckou sněmovnou. Pro usnesení hlasovalo 38 senátorek a senátorů z 52 přítomných, proti 2, zdrželo se 12 (hlasování č. 29).

20. Zákon byl doručen prezidentu republiky k podepsání dne 11. 6. 2008, který jej dne 25. 6. 2008 podepsal. Schválený zákon byl poté dne 30. 6. 2008 doručen k podpisu premiérovi. Zákon byl vyhlášen dne 4. 7. 2008 ve Sbírce zákonů v částce 78 pod č. 247/2008 Sb. s účinnosti od 1. 9. 2008.

21. Napadená vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, byla vydána Ministerstvem informatiky České republiky. Pravomoc ministerstev vydávat právní předpisy k provedení zákona je založena čl. 79 odst. 3 Ústavy České republiky. Materiálně je však podmíněná existencí výslovného zákonného zmocnění a jeho mezemi. V daném případě je tímto zmocněním právě napadené ustanovení § 97 odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích. Vyhláška byla podepsána ministryní pro informatiku a řádně publikována v částce 169 pod č. 485/2005 Sbírky zákonů s účinností dnem jejího vyhlášení, tj. 15. 12. 2005.

22. Ústavní soud konstatuje, že jak zákon č. 247/2008 Sb., kterým byla do zákona č. 127/2005 Sb., o elektronických komunikacích, vložena napadená ustanovení, tak napadená vyhláška č. 485/2005 Sb., byly přijaty Ústavou předvídaným způsobem.

V.
Dikce napadených ustanovení zákona a napadené vyhlášky

23. Napadená ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, znějí:

§ 97

(3) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje,

které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací[37b]). Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Právnická nebo fyzická osoba, která provozní a lokalizační údaje podle věty první a druhé uchovává, je na požádání povinna je bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu. Současně je tato osoba povinna zajistit, aby s údaji podle věty první a druhé nebyl uchováván obsah zpráv. Doba uchovávání těchto provozních a lokalizačních údajů nesmí být kratší než 6 měsíců a delší než 12 měsíců. Po uplynutí této doby je osoba, která údaje podle věty první a druhé uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního předpisu nebo tento zákon nestanoví jinak (§ 90).

(4) Rozsah provozních a lokalizačních údajů uchovávaných podle odstavce 3, dobu jejich uchovávání podle odstavce 3 a formu a způsob jejich předávání orgánům oprávněným k jejich využívání a dobu uchovávání a způsob likvidace údajů, které byly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu, stanoví prováděcí právní předpis.

[37b]) Směrnice 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.

24. Napadená vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, zní:

485/2005 Sb.
VYHLÁŠKA
ze dne 7. prosince 2005

o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání

Ministerstvo informatiky ve spolupráci s Ministerstvem vnitra stanoví podle § 150 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb. a zákona č. 361/2005 Sb., (dále jen "zákon") k provedení § 97 odst. 3 zákona:

§ 1

Pro účely této vyhlášky se rozumí
a) stanicí BTS základnová stanice veřejné mobilní telefonní sítě,

b) stanicí StartBTS základnová stanice veřejné mobilní telefonní sítě, do které je účastník alokován při zahájení komunikace,

c) stanicí StopBTS základnová stanice veřejné mobilní telefonní sítě, do které je účastník alokován při ukončení komunikace,

d) číslem IMEI mezinárodní identifikátor mobilního telefonního přístroje,

e) číslem MSISDN účastnické číslo ve veřejné mobilní telefonní síti,

f) číslem IMSI mezinárodní identifikátor účastníka veřejné mobilní telefonní sítě,

g) destinací určení sítě zahraničního operátora,

h) identifikátorem URI jednotný identifikátor zdroje,

i) kódem právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací se rozumí pořadové číslo osvědčení v evidenci podnikatelů podle § 14 zákona.

§ 2

Rozsah uchovávání provozních a lokalizačních údajů

(1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací (dále jen "provozovatel") poskytuje orgánu oprávněnému k jejich vyžádání (dále jen "oprávněný orgán") touto vyhláškou vymezené provozní a lokalizační údaje (dále jen "údaje").

(2) U sítí elektronických komunikací s přepojováním okruhů a pevným připojením se uchovávají

a) údaje o uskutečněné komunikaci s uvedením typu komunikace, telefonního čísla účastníka volajícího a volaného nebo identifikátoru telefonní karty pro použití ve veřejném telefonním automatu, data a času zahájení komunikace, délky komunikace, případně stavu komunikace,

b) údaje o všech veřejných telefonních automatech s uvedením jejich telefonního čísla, evidenčního čísla, geografické souřadnice a slovního popisu umístění.

(3) U veřejných mobilních telefonních sítí elektronických komunikací se uchovávají

a) údaje o uskutečněné komunikaci s uvedením typu komunikace, telefonního čísla účastníka volajícího a volaného, data a času zahájení komunikace, délky komunikace, čísla IMEI, čísla stanice StartBTS, popřípadě čísla stanice StopBTS, destinace a doplňkové informace,

b) údaje o vzájemných vazbách mezi čísly MSISDN a čísly IMEI společně použitými v síti, identifikace stanice BTS a čísla IMEI, které zprostředkovaly volání bez SIM karty na číslo tísňového volání "112", IP adresy terminálů, kterými bylo zprostředkováno odesílání zpráv SMS sítí Internet, datum a čas dobíjení kreditu u předplacených služeb, čísla dobíjecích kuponů k určitému telefonnímu číslu účastníka, telefonní číslo účastníka k určitému dobíjecímu kuponu,

c) údaje o všech stanicích BTS s uvedením jejich čísla, geografické souřadnice, azimutu směrování antén a slovního popisu umístění stanice BTS.

(4) U sítí elektronických komunikací s přepojováním paketů se uchovávají údaje o uskutečněné komunikaci

a) u služeb přístupu k síti s uvedením typu připojení, identifikátoru uživatelského účtu, identifikátoru zařízení uživatele služby, data a času zahájení připojení, data a času ukončení připojení, zájmových identifikátorů (například IP adresa, číslo portu), statusu události (například úspěch, neúspěch, řádné nebo mimořádné ukončení připojení), množství přenesených dat (v příchozím/v odchozím směru),

b) u služeb přístupu ke schránkám elektronické pošty s uvedením identifikátoru zájmového uživatelského zařízení, uživatelského účtu, identifikátoru zprávy na poštovním serveru, data a času zahájení komunikace, adresy elektronické pošty odesílatele, adres elektronické pošty příjemců, identifikátoru protokolu elektronické pošty, množství přenesených dat, informace o použití zabezpečené komunikace,

c) u služeb přenosu zpráv elektronické pošty s uvedením identifikátoru zájmového uživatelského zařízení, identifikátoru serveru elektronické pošty, data a času zahájení komunikace, adresy elektronické pošty odesílatele, adres elektronické pošty příjemců, identifikátoru protokolu elektronické pošty, množství přenesených dat, informace o použití zabezpečené komunikace,

d) u serverových služeb s uvedením identifikátoru zájmového uživatelského zařízení, identifikátoru uživatelského účtu, data a času požadavku na službu, veškerých identifikátorů serveru (zejména IP adresa, úplné doménové jméno FQDN), požadovaných identifikátorů URI nebo typu služby, dodatečných parametrů identifikátorů URI nebo služby, použité služby, množství přenesených dat, metody a statusu požadavku na službu,

e) u dalších služeb elektronických komunikací (zejména u služeb typu chat, usenet, instant messaging a IP telefonie) s uvedením veškerých identifikátorů komunikujících stran, transportního protokolu, data a času zahájení komunikace, data a času ukončení komunikace, použité služby, množství

přenesených dat.

§ 3

Způsob předávání údajů

(1) O poskytnutí uchovávaných údajů oprávněný orgán žádá provozovatele prostřednictvím svého určeného kontaktního pracoviště. Provozovatel vyžádané údaje bezodkladně předává prostřednictvím svého určeného kontaktního pracoviště. Údaje podle § 2 odst. 3 písm. c) se předávají souhrnně pravidelně jednou měsíčně v aktuálním stavu k datu předání.

(2) Komunikace mezi kontaktními pracovišti provozovatele a oprávněného orgánu probíhá přednostně způsobem umožňujícím dálkový přístup. Žádosti i údaje se předávají přednostně v elektronické podobě datových souborů. Při komunikaci kontaktních pracovišť se používá jen obecně dostupných technologií a komunikačních protokolů tak, aby řešení nebylo vázáno na určitého výrobce či dodavatele.

(3) Nelze-li použít pro komunikaci způsob umožňující dálkový přístup nebo bylo-li by použití takového způsobu neúčelné, lze předat žádost nebo vyžádané údaje v listinné podobě nebo v podobě datových souborů na přenosném médiu.

(4) K prokázání autentičnosti žádosti a předávaných údajů se použije

a) zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb[1]); k vytváření podpisu a jeho ověření se použije formát kryptografického standardu s veřejným klíčem PKCS#7,

b) průvodní dopis v listinné podobě obsahující číslo jednací nebo pořadové číslo žádosti, název souboru, datum, čas a způsob předání a případně i kontrolní součet nebo standardní hash souboru (například SHA-1) a podpis oprávněné osoby,

c) dopis v listinné podobě obsahující číslo jednací a podpis oprávněné osoby, nebo

d) v případě žádostí nebo údajů již předaných v elektronické podobě za určité období, zpravidla jednoho týdne, u nichž nebyl použit jiný způsob prokázání autentičnosti, dopis v listinné podobě obsahující číslo jednací a podpis oprávněné osoby, který se zasílá dodatečně.

(5) Údaje o komunikaci uskutečněné pod určitým identifikátorem za určité časové období provozovatel předává oprávněnému orgánu jako

a) výpis komunikace z pevné linky, jde-li o údaje podle § 2 odst. 2 písm. a),

b) výpis mobilní komunikace, jde-li o údaje podle § 2 odst. 3 písm. a),
c) výpis datové komunikace, jde-li o údaje podle § 2 odst. 4.

(6) Výpisy podle odstavce 5 se oprávněnému orgánu předávají ve strukturovaném textovém souboru, přednostně s kódováním podle znakové sady CP-1250, UTF-8 nebo ISO 8859-2. Soubory se zpracovávají samostatně ke každému jednotlivému telefonnímu číslu nebo jinému identifikátoru uvedenému v žádosti. Názvy předávaných souborů mají strukturu podle jmenné konvence uvedené v příloze.

(7) Soubor se uvozuje jednotnou hlavičkou a má pevnou strukturu stanovenou pro daný druh sítě nebo služby nebo typu požadavku. Jednotlivé řádky se v souboru řadí chronologicky, pokud v žádosti není uveden jiný parametr řazení. Výpis podle odstavce 5 je ukončen na posledním řádku slovem "Konec".

(8) Na řádku se jednotlivé údaje oddělují středníkem (kód 0059 znakové sady) nebo tabulátorem (kód 0009 znakové sady), poslední údaj se ukončuje znakem CRLF (kód 0013 a 0010 znakové sady). Pokud některý z údajů není požadován nebo prokazatelně není z použité technologie zjistitelný, jeho místo ve struktuře se ponechá prázdné.

(9) U údajů sestávajících z více hodnot se jednotlivé hodnoty oddělují znakem „\|“ (kód 0166 znakové sady). Pokud je součástí předávaných údajů znak shodný s některým z výše uvedených oddělovačů nebo znak „\“ (kód 0092 znakové sady), předřadí se před něj znak „\“ (například „\;“, „\CR\LF“, „\\“).

(10) V odůvodněných případech a se souhlasem oprávněného orgánu a provozovatele je možné použít formát, strukturu a název souboru odlišně od jejich vymezení v odstavcích 6 až 9.

§ 4
Doba uchovávání údajů
(1) Údaje se uchovávají po dobu 6 měsíců, není-li v odstavci 2 stanoveno jinak.

(2) Údaje uvedené v části 3 bodech 3.3.4.5 a 3.3.4.6 přílohy se uchovávají po dobu 3 měsíců.

§ 5
Účinnost
Tato vyhláška nabývá účinnosti dnem jejího vyhlášení, s výjimkou ustanovení § 4 odst. 2 a části 3 přílohy, která nabývají účinnosti dnem 1. prosince 2006.

Ministryně:
Ing. Bérová v. r.

---

[1]) *§ 11 zákona č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů*

VI.
Předběžná otázka

25. Předně Ústavní soud musel zvážit návrh předložený navrhovateli, aby předložil Evropskému soudnímu dvoru v souladu s čl. 234 Smlouvy o ES předběžnou otázku stran (ne)platnosti Směrnice o data retention, neboť existuje významné riziko, že samotná Směrnice o data retention, jež byla napadenými ustanoveními a napadenou vyhláškou transponována do českého právního řádu, je v rozporu s právem ES. V této souvislosti Ústavní soud zdůrazňuje, že i po přistoupení České republiky k EU (od 1. 5. 2004) zůstávají referenčním rámcem přezkumu Ústavního soudu normy ústavního pořádku České republiky, neboť úkolem Ústavního soudu je ochrana ústavnosti (čl. 83 Ústavy České republiky), a to v obou jejích aspektech, tj. jak ochrana objektivního ústavního práva, tak subjektivních, tj. základních práv. Komunitární právo není součástí ústavního pořádku, a proto není Ústavní soud příslušný k tomu, aby toto právo vykládal. Přesto Ústavní soud nemůže zcela přehlížet dopad komunitárního práva na tvorbu, aplikaci a interpretaci vnitrostátního práva, a to v oblasti právní úpravy, jejíž vznik, působení a účel je bezprostředně navázán na komunitární právo. [srov. k tomu nálezy Ústavního soudu sp. zn. Pl. ÚS 50/04 ze dne 8. 3. 2006 (N 50/40 SbNU 443; 154/2006 Sb.), sp. zn. Pl. ÚS 36/05 ze dne 16. 1. 2007 (N 8/44 SbNU 83; 57/2007 Sb.) či sp. zn. II. ÚS 1009/08 ze dne 8. 1. 2009 (N 6/52 SbNU 57)]. Obsah samotné Směrnice o data retenion však ponechává České republice dostatečný prostor pro její ústavně konformní transpozici do domácího právního řádu, když její jednotlivá ustanovení v podstatě pouze vymezují povinnost data uchovávat. Při transpozici je třeba dodržet účel, který Směrnice stanoví, avšak při zákonné a podzákonné konkrétní úpravě ukládání údajů a nakládání s nimi, včetně opatření bránících jejich zneužití, je třeba dodržet ústavní standard, který vyplývá z českého ústavního pořádku tak, jak je interpretován českým Ústavním soudem. To proto, že konkrétní podoba transpozice – tj. napadená zákonná a podzákonná ustanovení - je projevem vůle českého zákonodárce, jež při dodržení účelu Směrnice mohla co do výběru prostředků variovat, avšak zároveň byl při tomto výběru zákonodárce vázán ústavním pořádkem.

VII.
Referenční hlediska pro posouzení návrhu

VII. A) Právo na respekt k soukromému životu a právo na informační sebeurčení

26. V čl. 1 odst. 1 Ústavy České republiky je obsažen normativní princip demokratického právního státu. Základním atributem ústavního konceptu právního státu a podmínkou jeho fungování je respekt k základním právům a svobodám jednotlivce, který je, jako atribut zvoleného ústavního konceptu právního státu, v citovaném ústavním ustanovení výslovně vyjádřen. Toto ústavní ustanovení je bází materiálně chápané právní státnosti, kterou charakterizuje respekt veřejné moci ke svobodné (autonomní) sféře jednotlivce vymezené základními právy a svobodami a do této sféry veřejná moc zásadně nezasahuje, resp. zasahuje pouze v případech, které jsou odůvodněny kolizí s jinými základními právy, resp. ústavně aprobovaným a zákonem jednoznačně definovaným veřejným zájmem a za předpokladu, že je zákonem předvídaný zásah proporcionální jak s ohledem na cíle, jichž má být dosaženo, tak s ohledem na míru krácení omezovaného základního práva či svobody.

27. Koncept soukromí bývá nejčastěji spojován se západní kulturou a ještě přesněji s anglo-americkou kulturní představou zasazenou do politické filosofie liberalismu. Jde o koncept, který zjevně není obecně zcela sdílený jak v akcentu na význam soukromí, tak v rozsahu toho, co má být soukromím chráněno. V různých kulturách panují různé představy o tom, k jak rozsáhlému soukromí jsou jednotlivé osoby oprávněny a v jakých kontextech. Avšak již v roce 1928 píše soudce Brandeis v následně hojně citovaném disentu (k případu *Olmstead v. U.S.* 438, 478, 1928) následující hodnocení soukromí: „*Tvůrci naší Ústavy na sebe vzali odpovědnost vytvořit příznivé podmínky pro usilování o štěstí* (...) *Přiznali právo (proti státu) být ponechán „sám sobě“ – což je nejkomplexnější či nejobsažnější právo ze všech a zároveň i právo, které je nejvzácnější civilizovanému lidstvu.*“ A tak se z explicitně ústavně nezmíněného práva na soukromí postupem doby stal základní strukturální element U.S. ústavy, který zajišťuje autonomii jednotlivce, byť o jeho uplatnění je stále a opakovaně sváděna uvnitř U.S. Supreme Court bitva.

28. Požadavek respektu ke svébytnému uspořádání života se stal, vedle požadavku na respekt k vlastnímu životu, fyzické, psychické a duchovní integritě, osobní svobodě a k vlastnictví, centrálním lidskoprávním nárokem na autonomii jednotlivce, jež má formativní význam pro evropské vnitrostátní katalogy lidských (základních) práv, jakož i pro jejich pozdější regionální a univerzální pandány. Ani v evropských původních vnitrostátních katalozích základních práv však nebylo právo na soukromí či soukromý život jako takové explicitně zmiňováno, což dokládají texty národních ústav ještě ze 40. a 50. let minulého století (např. ústavy SRN, o Rakousku nemluvě, ústava Dánska, Finska, samozřejmě i Francie, jakož i Irska, ale také Itálie a dalších států). Požadavky respektu k soukromí a jeho ochrana jsou totiž úzce navázány na rozvoj technických a technologických možností, které samozřejmě zvyšují i svobodu ohrožující potenciál státu.

29. Jak Ústavní soud uvedl v nálezu sp. zn. II. ÚS 2048/09 ze dne 2. 11. 2009 (dostupný v el. databázi rozhodnutí http://nalus.usoud.cz): „*zcela zvláštní respekt a ochranu požívá v liberálních demokratických státech základní právo na nerušený soukromý život osoby (čl. 10 odst. 2 Listiny).*“ Primární funkcí práva na respekt k soukromému životu je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti. Vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů

(v manželství, v rodině, ve společnosti), právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst. 3 Listiny [srov. nálezy Ústavního soudu sp. zn. IV. ÚS 23/05 ze dne 17. 7. 2007 (N 111/46 SbNU 41) nebo sp. zn. I. ÚS 705/06 ze dne 1. 12. 2008 (N 207/51 SbNU 577), anebo rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1 (*Volkszählungsurteil*) či ze dne 4. 4. 2006, BVerfGE 115, 320 (*Rasterfahndungurteil II*)].

30. V citovaném rozhodnutí BVerfGE 65, 1, německý Spolkový ústavní soud při posouzení ústavnosti zákonné úpravy procesu sběru a uchovávání dat za účelem sčítání lidu (*Volkszählung*) mimo jiné konstatoval, že v moderní společnosti, charakterizované i obrovským nárůstem informací a dat, musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, užitím a zveřejňováním dat o její/jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce na soukromí. Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům; nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (*informationelle Selbstbestimmung*) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.

31. V Listině není právo na respekt k soukromému životu garantováno v jednom všezahrnujícím článku (jako je tomu v případu čl. 8 Úmluvy). Naopak, ochrana soukromé sféry jednotlivce je v Listině rozložena a doplňována dalšími aspekty práva na soukromí, deklarovanými na různých místech Listiny (např. čl. 7 odst. 1, čl. 10, čl. 12 a čl. 13 Listiny). Stejně tak i samotné právo na informační sebeurčení lze dovodit z čl. 10 odst. 3 Listiny, garantujícího jednotlivci právo na ochranu před neoprávněným shromažďováním, zveřejňováním a nebo jiným zneužíváním údajů o své osobě, a to ve spojení s čl. 13 Listiny, chránícím listovní tajemství a tajemství přepravovaných zpráv, ať již uchovávaných v soukromí, nebo zasílaných poštou, podávaných telefonem, telegrafem nebo jiným podobným zařízením anebo jiným způsobem. Nicméně onu „roztříštěnost“ právní úpravy aspektů soukromé sféry jednotlivce nelze přeceňovat a v Listině uvedený výčet toho, co je třeba podřadit pod „deštník“ práva na soukromí či na soukromý život nelze považovat za vyčerpávající a konečný. Při výkladu jednotlivých základních práv, která jsou zachycením práva na soukromí v jeho různých dimenzích tak, jak je uvádí Listina, je nezbytné respektovat účel obecně chápaného a dynamicky se vyvíjejícího práva na soukromí jako takového, resp. je třeba uvažovat o právu na soukromý život v jeho dobové celistvosti. Proto i právo na informační sebeurčení garantované čl. 10 odst. 3 a čl. 13 Listiny je třeba interpretovat zejména ve spojitosti s právy garantovanými čl. 7, čl. 8, čl. 10 a čl. 12 Listiny. Svou povahou i významem tak právo na informační sebeurčení spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní), svobodou komunikační a zajisté i dalšími ústavně garantovanými základními

právy, dotváří osobnostní sféru jedince, jehož individuální integritu, jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec, je nutno respektovat a důsledně chránit; zcela právem je proto respekt a ochrana této sféry garantována ústavním pořádkem, neboť - posuzováno jen z poněkud jiného úhlu - jde o výraz úcty k právům a svobodám člověka a občana (čl. 1 Ústavy ČR).

32. Z ustálené judikatury Ústavního soudu, zejména ve vztahu k problematice odposlechu telefonních hovorů, zřetelně vyplývá, že ochrana práva na respekt k soukromému životu v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny se vztahuje nejen k vlastnímu obsahu zpráv podávaných telefonem, ale i k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor [srov. např. nález sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001 (N 11/21 SbNU 83) – „*Soukromí každého člověka je hodno zásadní (ústavní) ochrany nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům. Lze tedy konstatovat, že čl. 13 Listiny zakládá i ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho trvání, v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor.* (...) *tyto údaje jsou nedílnou součástí komunikace uskutečněné prostřednictvím telefonu.*“ či obdobně nálezy sp. zn. IV. ÚS 78/01 ze dne 27. 8. 2001 (N 123/23 SbNU 197), sp. zn. I. ÚS 191/05 ze dne 13. 9. 2006 (N 161/42 SbNU 327) či sp. zn. II. ÚS 789/06 ze dne 27. 9. 2007 (N 150/46 SbNU 489)].

33. Ústavní soud v citovaných nálezech vycházel i z judikatury ESLP [zejména rozhodnutí ve věci *Malone proti UK* (no. 8691/79 ze dne 2. 8. 1984)], který z čl. 8 Úmluvy, garantujícího právo na respekt k soukromému a rodinnému životu, jakož i k obydlí a ke korespondenci, dovodil i právo na informační sebeurčení, když několikrát zdůraznil, že sběr a uchovávání údajů týkajících se soukromého života jednotlivce spadají pod rozsah čl. 8 Úmluvy, neboť výraz "soukromý život" nesmí být interpretován restriktivně. Tato fazeta práva na soukromí tak konzumuje i právo na ochranu před sledováním, hlídáním a pronásledováním ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech. Navíc žádný zásadní důvod neumožňuje vyloučit z pojmu soukromého života aktivity profesní, obchodní či sociální [srov. rozhodnutí ve věci *Niemietz proti Německu* (no. 13710/88) ze dne 16. 12. 1992]. Jak uvedl ESLP, tato extenzivní interpretace pojmu „soukromý život“ je ve shodě s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních údajů (vypracovanou Radou Evropy k 28. 1. 1981, v České republice v platnosti od 1. 11. 2001, publ. pod č. 115/2001 Sb. m. s.), jejímž cílem je "*zaručit na území každé smluvní strany každé fyzické osobě (...) respektování jejích práv a základních svobod, a zejména jejího práva na soukromý život, v souvislosti s automatizovaným zpracováním údajů osobního charakteru, které se jí týkají (čl. 1), přičemž ty jsou definovány jako jakékoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby" (čl. 2).*“ [srov. rozhodnutí ve věci *Amman proti Švýcarsku* (no. 27798/95) ze dne 16. 2. 2000 a tam citovaná judikatura].

34. ESLP ve své judikatuře k právu na respekt k soukromému životu dle čl. 8 Úmluvy označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů [srov. rozhodnutí ve věci *Klass a další proti Německu* (no. 5029/71) ze dne 6. 9. 1978, rozhodnutí ve věci *Leander proti Švédsku* (no. 9248/81) ze dne 26. 3. 1987, rozhodnutí ve věci *Kruslin proti Francii* (no.11801/85) ze dne 24. 4. 1990 či rozhodnutí ve věci *Kopp proti Švýcarsku* (no. 23224/94) ze dne 25. 3. 1998], zjišťování telefonních čísel telefonujících osob [srov. rozhodnutí ve věci *P. G. a J. H. proti*

UK (no. 44787/98) ze dne 25. 9. 2001], zjišťování údajů o telefonním spojení (srov. cit. rozhodnutí ve věci *Amman proti Švýcarsku*) nebo uchovávání údajů o DNA jednotlivců v databázích obviněných [srov. rozhodnutí ve věci *S. a Marper proti UK* (no. 30562/04 a 30566/04) ze dne 4. 12. 2008]. V rozhodnutí ve věci *Rotaru proti Rumunsku* (no. 28341/95) ze dne 4. 5. 2000 ESLP dovodil z práva na soukromý život projevujícího se v podobě práva na informační sebeurčení i pozitivní povinnost státu, zlikvidovat data, která o osobě z její soukromé sféry stát shromáždil a zpracoval.

35. Obdobný přístup zastává i judikatura zahraničních ústavních soudů. Např. zmíněný Spolkový ústavní soud SRN prostřednictvím práva na informační sebeurčení garantuje ochranu nejen obsahu předávaných informací, ale chrání i vnější okolnosti, za nichž se uskutečňují – tj. místo, čas, účastníky, druh a způsob komunikace, neboť znalost okolností uskutečněné komunikace může ve spojení s dalšími údaji sama o sobě indikovat samotný obsah komunikace a za pomoci zkoumání těchto údajů a jejich analýzy lze zhotovit individuální profily účastníků dané komunikace. (srov. k tomu např. rozhodnutí ze dne 27. 7. 2005, BVerfGE 113, 348 (*Vorbeugende Telekommunikationsüberwachung*) či ze dne 27. 2. 2008, BVerfGE 120, 274 (*Grundrecht auf Computerschutz*).

VII. B) Přípustnost zásahu do práva na informační sebeurčení

36. Za primární cíl právní regulace plošného a preventivního sběru a uchovávání provozních a lokalizačních údajů o elektronické komunikaci bývá obecně označována ochrana před bezpečnostními hrozbami a potřeba zajištění dostupnosti těchto údajů pro účely předcházení, odhalování, vyšetřování a stíhání závažných trestných činů ze strany veřejné moci. Jak již Ústavní soud v minulosti několikrát zdůraznil, stíhání trestných činů a spravedlivé potrestání jejich pachatelů je ústavně aprobovatelným veřejným zájmem, jehož podstatou je přenesení odpovědnosti za postihování nejzávažnějších porušování základních práv a svobod fyzickými a právnickými osobami na stát. Umožňuje-li trestní právo realizaci veřejného zájmu na stíhání trestné činnosti pomocí robustních nástrojů, jejichž užití má za následek vážné omezení osobní integrity a základních práv a svobod jednotlivce, pak při jejich aplikaci musí být respektovány ústavněprávní limity. K omezení osobní integrity a soukromí osob (tj. k prolomení respektu k nim) tak ze strany veřejné moci může dojít jen zcela výjimečně, je-li to v demokratické společnosti nezbytné, nelze-li účelu sledovaného veřejným zájmem dosáhnout jinak, a je-li to akceptovatelné z pohledu zákonné existence a dodržení účinných a konkrétních záruk proti libovůli. Esenciální předpoklady spravedlivého procesu totiž vyžadují, aby byl jednotlivec vybaven dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci. Ony nezbytné záruky se sestávají z odpovídající právní úpravy a z existence účinné kontroly jejich dodržování, kterou představuje především kontrola těch nejintenzivnějších zásahů do základních práv a svobod jednotlivců nezávislým a nestranným soudem, neboť je povinností soudů poskytovat ochranu základním právům a svobodám jednotlivců (čl. 4 Ústavy České republiky) [srov. nálezy sp. zn. I. ÚS 631/05 ze dne 7. 11. 2006 (N 205/43 SbNU 289) a sp. zn. Pl. ÚS 3/09 ze dne 8. 6. 2010 (219/2010 Sb., dostupný v el. databázi rozhodnutí http://nalus.usoud.cz)].

37. Naplnění výše předestřených podmínek pak Ústavní soud ve své judikatuře blíže konkretizoval při posuzování přípustnosti zásahu veřejné moci do soukromí jednotlivců v podobě užití odposlechů telekomunikačního provozu [srov. např. cit. nálezy sp. zn. II. ÚS 502/2000, sp. zn. IV. ÚS 78/01, sp. zn. I. ÚS 191/05 či nález sp. zn. I. ÚS 3038/07 ze dne 29. 2. 2008 (N 46/48 SbNU 549)]. Zásah do základního práva jednotlivce na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny z důvodu

prevence a ochrany před trestnou činností je tak možný jen skrze imperativní zákonnou úpravu, která musí především odpovídat nárokům plynoucím z principu právního státu a která naplňuje požadavky vyplývající z testu proporcionality, kdy v případech střetů základních práv či svobod s veřejným zájmem, resp. s jinými základními právy či svobodami je třeba posuzovat účel (cíl) takového zásahu ve vztahu k použitým prostředkům, přičemž měřítkem pro toto posouzení je zásada proporcionality (v širším smyslu). Taková právní úprava musí být přesná a zřetelná ve svých formulacích a dostatečně předvídatelná, aby potenciálně dotčeným jednotlivcům poskytovala dostatečnou informaci o okolnostech a podmínkách, za kterých je veřejná moc oprávněna k zásahu do jejich soukromí a případně tak mohli upravit své chování tak, aby se nedostali do konfliktu s omezující normou. Rovněž musí být striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování. Posouzení přípustnosti daného zásahu z hlediska zásady proporcionality (v širším smyslu) pak zahrnuje tři kritéria. Prvním z nich je posouzení způsobilosti naplnění účelu (nebo také vhodnosti), přičemž je zjišťováno, zda je konkrétní opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se pak jedná o posouzení potřebnosti, v němž je zkoumáno, zda byl při výběru prostředků použit ten prostředek, který je k základnímu právu nejšetrnější. A konečně je zkoumána přiměřenost (v užším smyslu), tj. zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl, tzn. že opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky převyšovat pozitiva, která představuje veřejný zájem na těchto opatřeních. [srov. nález sp. zn. Pl. ÚS 3/02 ze dne 13. 8. 2002 (N 105/27 SbNU 177; 405/2002 Sb.)].

38. Nezbytný požadavek soudní ochrany základních práv se v případě užití trestněprávních nástrojů omezujících základní práva a svobody jednotlivce projevuje zejména ve vydání soudního příkazu a v jeho dostatečném odůvodnění. To musí odpovídat jak požadavkům zákona, tak především ústavním principům, z nichž zákonné ustanovení vychází, resp. které zpětně limitují jeho interpretaci, neboť aplikace takového ustanovení představuje zvlášť závažný zásah do základních práv a svobod každého jednotlivce. „*Soudní příkaz k odposlechu a záznamu telekomunikačního provozu může být vydán jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost, a musí být podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání takového trestného činu. Příkaz musí být individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice. Konečně musí příkaz alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny, a z čeho je to vyvozováno.*“ (srov. cit. nálezy Ústavního soudu sp. zn. II. ÚS 789/06 či sp. zn. I. ÚS 3038/07).

39. Obdobný přístup zastává i ESLP ve své judikatuře. ESLP tak v souladu s čl. 8 odst. 2 Úmluvy, jenž vymezuje ústavněprávní limity omezení základních práv a svobod jednotlivců garantovaných čl. 8 odst. 1 Úmluvy, v každém jednotlivém případě předně posuzuje, zda tvrzený zásah či omezení základních práv či svobod je podřaditelné pod rozsah ochrany čl. 8 Úmluvy. Pokud ano, byl-li tvrzený zásah do práva na soukromí ze strany veřejné moci proveden v souladu se zákonem, jenž musí být dostupný a dostatečně předvídatelný, tedy vyjádřený s velkou mírou přesnosti tak, aby jednotlivci dovolil v případě potřeby regulovat své chování (srov. *Malone proti UK*, *Amman proti Švýcarsku* či *Rotaru proti Rumunsku*). Úroveň přesnosti požadované po vnitrostátní právní úpravě, která v žádném případě nemůže počítat se všemi eventualitami, do značné míry závisí na obsahu zkoumaného textu, na oblasti, kterou má pokrývat a počtu a statusu osob, kterým je určena

[*Hassan a Tchaouch proti Bulharsku* (no. 30985/96, 39023/97) ze dne 26. 10. 2000]. Přezkoumávaný zásah do základních práv či svobod garantovaných čl. 8 odst. 1 Úmluvy musí ve smyslu čl. 8 odst. 2 Úmluvy být rovněž nezbytným v demokratické společnosti, sledovat Úmluvou aprobovaný účel (např. ochrana života nebo zdraví osob, národní a veřejné bezpečnosti, ochrana práv a svobod druhých či morálky, předcházení nepokojům a zločinnosti či zájem na hospodářském blahobytu země), který musí být relevantní a řádně odůvodněný. Aby bylo možné zákonnou úpravu posoudit jako souladnou s Úmluvou, musí ve smyslu čl. 13 Úmluvy rovněž poskytovat přiměřenou ochranu proti svévoli a v důsledku toho s dostatečnou jasností definovat rozsah a způsob výkonu pravomocí svěřených kompetentním orgánům (srov. *Kruslin proti Francii* či *S. a Marper proti UK*). Jinými slovy, úkony představující očividný zásah do základního práva na soukromý život se nesmí ocitnout mimo jakoukoli bezprostřední (preventivní či následnou) soudní kontrolu [srov. např. rozhodnutí věci *Camenzind proti Švýcarsku* (no. 21353/93) ze dne 16. 12. 1997].

40. ESLP zmíněné požadavky na právní úpravu umožňující zásah do práva na soukromý život blíže konkretizoval v těch výše uvedených rozhodnutích, v nichž posuzoval přípustnost takového zásahu ze strany veřejné moci v podobě užití odposlechu telefonních hovorů, tajného dohledu, sběru informací a dat ze soukromé (osobnostní) sféry jednotlivce. ESLP zdůraznil, že je předně nutné vymezit jasná a detailní pravidla upravující rozsah a použití takových opatření, stanovit minimální požadavky na délku, způsob uložení získaných informací a údajů, jejich použití, přístup třetích osob k nim, a zakotvit procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a rovněž k jejich ničení, a to způsobem, aby jednotlivci disponovali dostatečnými zárukami proti riziku jejich zneužití a svévole. Nezbytnost disponovat takovými zárukami je o to větší, když se jedná o ochranu osobních údajů podrobených automatickému zpracování, zejména pokud jsou tyto údaje využívané k policejním cílům a v situaci, kdy se dostupné technologie stávají stále komplikovanějšími. Vnitrostátní právo musí zejména zaručit, že shromážděné údaje jsou skutečně relevantní a nejsou přehnané vzhledem k účelu, pro který byly zajištěny a dále, že jsou uchovávány ve formě umožňující identifikaci osob během doby nepřesahující nezbytnou míru k dosažení účelu, pro který byly zajištěny [srov. Preambule a čl. 5 Úmluvy o ochraně dat a zásada č. 7 Doporučení Výboru ministrů č. R(87)15 ze dne 17. 9. 1987 týkající se úpravy a využití osobních údajů v policejním sektoru, cit. dle rozhodnutí ve věci *Weber a Saravia proti Německu* (no. 54934/00) ze dne 29. 6. 2006 či *Liberty a další proti UK* (no. 58243/00) ze dne 1. 7. 2008].

VIII. Vlastní přezkum

VIII. A) Tzv. data retention

41. Jak již Ústavní soud výše zmínil, napadená ustanovení § 97 odst. 3 a 4 se stala součástí zákona č. 127/2005 Sb., o elektronických komunikacích, na základě zákona č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Dle důvodové zprávy přijetí této novely sloužilo k implementaci „*některých článků*“ Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 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, „*které doposud nejsou do našeho právního řádu implementovány, či jsou implementovány jen částečně,* (neboť) *Směrnice o data retention je v České republice již transponována* (...). *Platná právní úprava je v některých ohledech širší než úprava obsažená ve Směrnici o data retention*.“ Problematika uchovávání provozních a lokalizačních údajů je totiž v českém právním řádu v pozměněné podobě upravena již od přijetí samotného

zákona č. 127/2005 Sb., o elektronických komunikacích, s účinností od 1. 5. 2005, a od přijetí napadené vyhlášky Ministerstva informatiky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, s účinností od 15. 12. 2005. V dané době v EU pouze připravovaná Směrnice o data retention tak skutečně byla v České republice fakticky implementována s předstihem a samotné znění napadených ustanovení již dle požadavků Směrnice o data retention pouze představuje upřesnění povinnosti uchovávat provozní a lokalizační údaje a tyto údaje bezodkladně poskytovat orgánům oprávněným k jejich vyžádání. Napadená vyhláška Ministerstva informatiky navzdory této skutečnosti již ovšem změněna nebyla, což má za následek tu skutečnost, že se napadenou právní úpravou regulovaný rozsah uchovávaných údajů i nadále zcela zřetelně pohybuje nad rámcem rozsahu předvídaného předmětnou Směrnicí o data retention.

42. Podle napadeného ust. § 97 odst. 3 věty prvé a druhé zákona o elektronických komunikacích právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací, a to včetně údajů o neúspěšných pokusech o volání, jsou-li i tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Dle § 90 zákona o elektronických komunikacích se provozními údaji rozumí „*jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.*“ Dle § 91 téhož zákona se za lokalizační údaje považují „*jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.*“ Konkretizaci a samotný rozsah provozních a lokalizačních údajů, dobu jejich uchovávání a formu a způsob jejich předávání orgánům oprávněným k jejich využívání pak dle napadeného ust. § 97 odst. 4 má vymezovat prováděcí právní předpis, kterým je napadená vyhláška č. 485/2005 Sb.

43. Konkrétně u služeb pevných telefonních linek a mobilní komunikace jsou provozovatelé povinni shromažďovat prakticky všechny dostupné údaje o uskutečněných hovorech i (pokud jsou zaznamenávány) o jejich neúspěšných pokusech (typicky „prozvánění“). Jedná se zejména o údaje o typu uskutečněné komunikace, o telefonních číslech volajícího a volaného, o datu a času zahájení a ukončení komunikace, označení základové stanice, která zajišťovala hovor v okamžiku spojení, identifikaci předplacené telefonní karty, veřejného telefonního automatu, u mobilní komunikace navíc data o jednoznačném kódu používaného k identifikaci každého mobilního telefonu, který je používán v rámci GSM sítě (IMEI), o jeho poloze a pohybu, a to i pokud komunikace neprobíhá (stačí zapnutý mobilní telefon), čísla dobíjecích kuponů a jejich přiřazení k dobíjenému číslu, vazbu mezi mobilním přístrojem a všemi vloženými SIM kartami aj. Ještě větší objem a rozsah dat a údajů, které dle napadené právní úpravy musí být uchovávány, se vztahují k tzv. veřejným sítím, fungujícím na principu přepojování paketů a jejich služeb, nejtypičtěji internetu. V případě jeho použití je napadenou právní úpravou vyžadováno uchovávání údajů zejména o přístupu k síti (např. čas, místo a délka připojení, údaje o uživatelích a jejich uživatelských účtech, identifikátor počítače i serveru, k němuž bylo přistupováno, IP adresa, úplné doménové jméno, objem přenesených dat, aj.), dále údaje vztahující se k přístupu ke schránkám elektronické pošty a přenosu zpráv elektronické pošty (v tomto případě jsou uchovávány prakticky veškeré údaje kromě obsahu samotných zpráv, tj. včetně identifikace adres, objemu přenesených dat aj.), a v neposlední řadě i údaje

o serverových a ostatních službách [např. zadané URL adresy, druh požadavku, údaje o použití chatu, usenetu, instant messagingu (např. ICQ) a IP telefonie, a to včetně identifikace komunikujících stran, doby a použité služby (např. přenos souborů či transakce)]. Nad rámec předmětné Směrnice o data retention se u internetového připojení a služeb a e-mailové komunikace sleduje a uchovává množství přenesených dat, informace o použití šifrování, metoda a status požadavků na službu a její realizace a rovněž i informace o posílání SMS z internetových bran a další „zájmové identifikátory". U telefonie nad rámec Směrnice o data retention napadená právní úprava vyžaduje uchovávat údaje o identifikaci předplacené telefonní karty, veřejného telefonního automatu, číslech dobíjecích kuponů a jejich přiřazení k dobíjenému číslu, vazbách mezi mobilním přístrojem a vloženými SIM kartami.

44. Ačkoliv se stanovená povinnost uchovávat provozní a lokalizační údaje nevztahuje na obsahy jednotlivých sdělení (viz čl. 1 odst. 2 Směrnice o data retention a napadené ust. § 97 odst. 3 věta čtvrtá), z uvedených údajů o uživatelích, adresátech, přesných časech, datech, místech a formách telekomunikačních spojení, budou-li sledovány po delší časový úsek, lze v jejich kombinaci sestavit detailní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob. Ve výše rekapitulovaném vyjádření Senátu předestřený názor předkladatele návrhu zákona, že se „*v žádném případě nejedná o něco, co by se dalo přirovnat k odposlechům, už jen proto, že se neuchovávají obsahy jednotlivých telefonátů nebo mailových zpráv*", je zcela mylný, neboť i pouze na jejich základě lze učinit dostatečné obsahové závěry spadající do soukromé (osobnostní) sféry daného jednotlivce. Z uvedených údajů lze až s 90% jistotou např. dovodit, s kým, jak často a dokonce v jakých hodinách se daný jednotlivec stýká, kdo jsou jeho nejbližší známí, kamarádi či kolegové z práce anebo jaké aktivity a v jakých hodinách provozuje [srov. studii Massachusetts Institute of Technology (MIT), *Relationship Inference*, dostupnou na http://reality.media.mit.edu/dyads.php]. Sběr a uchovávání lokalizačních a provozních údajů tak rovněž představuje významný zásah do práva na soukromí a z toho důvodu je nezbytné pod rozsah ochrany základního práva na respekt k soukromému životu v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny) zahrnout nejen ochranu vlastního obsahu zpráv podávaných prostřednictvím telefonní komunikace či komunikace prostřednictvím tzv. veřejných sítí, ale i provozní a lokalizační údaje o nich.

VIII. B) Posouzení napadené právní úpravy z hlediska ústavněprávních požadavků

45. Ústavní soud tak musel posoudit, zda napadená právní úprava, jíž je regulována problematika plošného a preventivního sběru a uchovávání stanovených provozních a lokalizačních údajů o elektronické komunikaci (tzv. *data retention*), odpovídá výše předestřeným ústavněprávním požadavkům na právní úpravu umožňující zásah do základních práv jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny). Navíc s ohledem na intenzitu takového zásahu, která je v daném případě zvýrazněna tím, že se dotýká obrovského a nepředvídatelného počtu účastníků komunikace, neboť se jedná o plošný a preventivní sběr a uchovávání předmětných údajů, bylo nutné na splnění uvedených požadavků klást co nejpřísnější měřítka. Ústavní soud přitom dospěl k závěru, že napadená právní úprava výše předestřeným ústavněprávním požadavkům zdaleka neodpovídá, a to hned z několika důvodů.

46. Napadené ustanovení § 97 odst. 3 věta třetí zákona o elektronických komunikacích obsahuje pouze vágní a zcela neurčité stanovení povinnosti právnickým nebo fyzickým osobám, které ve výše uvedeném rozsahu provozní a lokalizační údaje uchovávají,

„*na požádání je bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu.*“ Ačkoliv napadená vyhláška v § 3 konkretizuje, jakým způsobem dochází v jednotlivých případech ke splnění této povinnosti vůči oprávněným orgánům, tj. relativně velmi podrobně vymezuje způsob předávání údajů, způsob komunikace (elektronicky), formát, užívané programy, kódy atd., přesto ze samotného znění napadeného ustanovení § 97 odst. 3 zákona o elektronických komunikacích, ba ani z důvodové zprávy dle názoru Ústavního soudu zřetelně nevyplývá, o jaké oprávněné orgány a o jaké zvláštní právní předpisy se konkrétně jedná. S ohledem na znění ust. § 97 odst. 1 zákona o elektronických komunikacích, jež právnickým nebo fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací stanovuje povinnost na náklady žadatele zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, lze jen předpokládat, že se i v případě povinnosti předávat uchovávané provozní a lokalizační údaje jedná o stejné oprávněné orgány a o podobné zvláštní právní předpisy, jejichž adresátem jsou orgány činné v trestním řízení, patrně dle § 88a tr. řádu, Bezpečnostní informační služba, dle §§ 6 až 8a zákona č. 154/1994 Sb., o Bezpečnostní informační službě, a Vojenské zpravodajství dle §§ 9 a 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství. Takto vymezená právní úprava umožňující masivní zásah do základních práv nesplňuje požadavky kladené na určitost a jasnost z pohledu právního státu (viz bod 37).

47. Stejně tak není zcela jasně a přesně vymezen účel, za jakým jsou provozní a lokalizační údaje oprávněným orgánům poskytovány, což znemožňuje posouzení napadené úpravy z hlediska její skutečné potřebnosti (když je jistě způsobilá naplnit účel, resp. je schopná dosáhnout cíle stanoveného Směrnicí – viz dále). Zatímco citovaná Směrnice o data retention v čl. 1 odst. 1 zřetelně vymezuje, že byla přijata za účelem harmonizace předpisů členských států, které se týkají povinností poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, pokud jde o uchovávání provozních a lokalizačních údajů, které jsou nezbytné k identifikaci účastníka či registrovaného uživatele, s cílem „*zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů*,“ (byť blíže nedefinuje, o jaké trestné činy se jedná), neobsahuje napadená právní úprava, a dokonce ani citované ust. § 88a odst. 1 tr. řádu, upravující podmínky použití uchovávaných údajů pro účely trestního řízení, žádné takové omezení. Možnost použití uchovávaných údajů v trestním řízení tak, dle předmětné právní úpravy, není zákonodárcem nijak vázána na důvodné podezření ze spáchání závažného trestného činu, stejně jako není upravena povinnost orgánů činných v trestním řízení o této skutečnosti dotčenou (sledovanou) osobu, byť i následně informovat, čímž nesplňuje nároky vyplývající z druhého kroku testu proporcionality, tj. potřebnosti při výběru prostředků, neboť z uvedeného je zřejmé, že nebyl použit ten prostředek, který je k základnímu právu na informační sebeurčení osob nejšetrnější.

48. Uvedený způsob (ne)vymezení spektra oprávněných orgánů veřejné moci, jakož i (ne)vymezení účelu, pro který jsou uchovávané údaje oprávněny požadovat, Ústavní soud nepovažuje za dostatečný a předvídatelný. Ačkoliv dle cit. ustanovení § 88a odst. 1 tr. řádu použití uchovávaných údajů podléhá soudní kontrole, a to v podobě vydání povolení ze strany předsedy senátu (a v přípravném řízení soudce), bylo primárně povinností zákonodárce, aby v napadených ustanoveních anebo v cit. ust. § 88a odst. 1 tr. řádu namísto zcela neurčitého vymezení podmínky použití uchovávaných údajů „*o uskutečněném telekomunikačním provozu*“ za účelem „*objasnění skutečností důležitých pro trestní řízení*“ zřetelněji a jednoznačněji stanovil, jak předpoklady a podmínky pro jejich použití, tak

i rozsah jejich použití. Zejména je nezbytné, aby s ohledem na závažnost a míru zásahu do základního práva jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny), jež použití uchovávaných údajů představuje, zákonodárce omezil možnost použití uchovávaných údajů jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy a jen pro případ, že nelze sledovaného účelu dosáhnout jinak. Tak to ostatně předpokládá nejen citovaná Směrnice o data retention, ale i ust. § 88 odst. 1 tr. řádu upravující podmínky pro nařízení odposlechu a záznamu telekomunikačního provozu („*je-li vedeno trestní řízení pro zvlášť závažný trestný čin*"), od níž se zmíněná právní úprava ust. § 88a tr. řádu jako celek (navzdory právním názorům Ústavního soudu obsaženým v citovaných nálezech sp. zn. II. ÚS 502/2000 či sp. zn. IV. ÚS 78/01) zcela bezdůvodně odchyluje a normuje úpravu, která je ve zřetelném rozporu s názory Ústavního soudu.

49. Absence řádné ve smyslu ústavně konformní právní úpravy, jak ostatně vyplývá ze statistických údajů, má v praxi za následek, že nástroj v podobě vyžádání si a použití uchovávaných údajů (včetně údajů o neuskutečněných hovorech, na které trestní řád vůbec nepamatuje) je orgány činnými v trestním řízení využíván (nadužíván) pro účely vyšetřování i běžné, tj. méně závažné trestné činnosti. Tak např. dle „*Zprávy o bezpečnostní situaci v ČR za období roku 2008*" bylo na území České republiky zjištěno celkem 343 799 trestných činů, z toho bylo objasněno 127 906 trestných činů, přičemž ve stejném období počet žádostí o poskytnutí provozních a lokalizačních údajů ze strany oprávněných orgánů veřejné moci dosáhl čísla 131 560. (srov. k tomu zprávu Komise EU – „*The Evaluation of Directive 2006/24/EC and National Measures to Combat criminal Misuse and Anonymous Use of Electronic Data*", která si oficiální údaje od české strany vyžádala, přičemž reakce zástupců České republiky na otázky v dotazníku ze dne 30. 9. 2009 jsou dostupné na http://www.dataretention2010.net/docs.jsp). Následně, a to jen za období od ledna do října 2009 byla dle neoficiálních údajů žádost o poskytnutí lokalizačních a provozních údajů učiněna již ve 121 839 případech (srov. k tomu Herczeg, J.: *Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou*, Bulletin advokacie č. 5/2010, s. 29).

50. Navrhovateli napadená právní úprava dle názoru Ústavního soudu rovněž zcela nedostatečně, příp. vůbec nestanovuje jasná a detailní pravidla obsahující minimální požadavky na zabezpečení uchovávaných údajů, zejména v podobě zamezení přístupu třetích osob, stanovení procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a procedury jejich ničení. Dále je třeba napadené úpravě vytknout, že dotčení jednotlivci nedisponují dostatečnými zárukami proti riziku zneužití údajů a svévole. Nezbytnost disponovat takovými zárukami se přitom v posuzovaném případě plošného a preventivního sběru a uchovávání údajů v rámci elektronické komunikace stává pro jednotlivce naléhavější právě v dnešní době, kdy díky enormnímu rozvoji a výskytu nových a komplikovanějších informačních technologií, systémů a komunikačních prostředků nevyhnutelně dochází k plynulému posunu hranice mezi privátním a veřejným prostorem, a to ve prospěch veřejné sféry, neboť ve virtuálním prostoru informačních technologií a elektronické komunikace (v tzv. kyberprostoru) jsou, zejména díky rozvoji internetu a mobilní komunikace, každou minutou zaznamenávány, shromažďovány a fakticky zpřístupněny tisíce, ba miliony dat, údajů a informací, které zasahují i do soukromé (osobnostní) sféry každého jednotlivce, ačkoliv on sám do ní vědomě nikoho vpustit nechtěl.

51. Ústavní soud za dostatečně jasné, podrobné a adekvátní záruky v žádném případě nepovažuje pouhé zakotvení povinnosti uložené právnickým nebo fyzickým osobám zajistit,

„*aby s vymezenými uchovávanými údaji nebyl uchováván i obsah zpráv*“ (§ 97 odst. 3 věta čtvrtá), resp. povinnosti je „*po uplynutí doby zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu nebo tento zákon nestanoví jinak (§ 90)*“ (§ 97 odst. 3 věta šestá). Za nejednoznačné a vzhledem k rozsahu a citlivosti uchovávaných údajů za zcela nedostačující lze již označit vymezení samotné doby jejich uložení, a to v rozmezí „*ne kratší než 6 měsíců a delší než 12 měsíců*“, od jejíhož uplynutí se odvíjí povinnost uvedené údaje zlikvidovat. U žádné z uvedených povinností nejsou nijak detailněji popsána pravidla a konkrétní postupy jejich plnění, nejsou striktně vymezeny požadavky na zabezpečení uchovávaných údajů, není dostatečně seznatelné, jak je s uvedenými údaji nakládáno, ať už samotnými právnickými nebo fyzickými osobami, které provozní a lokalizační údaje uchovávají, anebo po jejich vyžádání oprávněnými orgány veřejné moci, stejně jako není konkrétně stanoven způsob jejich likvidace. Rovněž není nijak definována odpovědnost a případné sankce za nesplnění takových povinností, včetně absence zakotvení možnosti dotčených jednotlivců, domáhat se efektivní ochrany proti případnému zneužití, svévoli či nesplnění stanovených povinností. Zákonem o elektronických komunikacích (§ 87 a násl.) předvídaný dozor Úřadu pro ochranu osobních údajů „*nad dodržováním povinností při zpracování osobních údajů*“ a vymezené nástroje jeho činnosti a kontroly nelze považovat za adekvátní a efektivní prostředek k ochraně základních práv dotčených jednotlivců, neboť tento nástroj neovládají sami [viz přiměřeně nález sp. zn. Pl. ÚS 15/01 ze dne 31. 10. 2001 (N 164/24 SbNU 201; 424/2001 Sb.)]. Uvedené úkony, představující očividný zásah do základního práva jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny), se tak vlivem nedostatečné a shora uvedeným ústavněprávním požadavkům neodpovídající právní úpravy ocitají mimo jakoukoliv bezprostřední, byť i následnou kontrolu, zejména pak kontrolu soudní, k jejíž nezbytnosti se vyjádřil i ESLP v citovaném rozhodnutí *Camenzind v. Švýcarsko*.

52. K obdobným závěrům dospěly i ústavní soudy v jiných evropských státech, které rovněž přezkoumávaly ústavnost právní úpravy implementující citovanou Směrnici o data retention. Např. Spolkový ústavní soud SRN v rozhodnutí ze dne 2. března 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, napadenou právní úpravu regulující problematiku preventivního uchovávání dat (*Vorratsdatenspeicherung*) (ve smyslu §§ 113a, 113b *Telekommunikationsgesetz*) a jejich užití v rámci trestního řízení (ve smyslu § 100g odst. 1 *Strafprozessordnung*) shledal protiústavní pro rozpor s čl. 10 odst. 1 Základního zákona, jenž garantuje nedotknutelnost listovního, poštovního a telekomunikačního tajemství. Spolkový ústavní soud SRN konstatoval, že napadená právní úprava neodpovídá požadavkům plynoucím ze zásady proporcionality, která mj. vyžaduje, aby zákonná úprava ukládání dat odpovídala zvláštní závažnosti tohoto zásahu do základních práv jednotlivců. Konkrétně, napadená právní úprava dostačujícím způsobem nevymezovala účel použití těchto dat, nezaručovala jejich dostatečné zabezpečení a v neposlední řadě jednotlivci dostatečně negarantovala adekvátní a efektivní záruky proti riziku zneužití, zejména v podobě soudní kontroly. Ke splnění těchto požadavků byl dle čl. 73 odst. 1, bod 7 Základního zákona povolán spolkový zákonodárce. K obdobným závěrům dospěl i rumunský Ústavní soud v rozhodnutí ze dne 8. 10. 2009 (č. 1258), který tamní právní úpravu označil za protiústavní, neboť dostatečně nevymezovala účel použití takového nástroje, její znění bylo příliš vágní, aniž by blíže vymezovala pravomoci a povinnosti oprávněných orgánů veřejné moci, a dotčeným jednotlivcům neposkytovala, díky absenci soudní kontroly, dostatečné záruky proti zneužití (rozhodnutí v neoficiálním anglickém překladu dostupné na http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian constitutional-court-decision-regarding-data-retention.html), dále bulharský Nejvyšší správní soud v rozhodnutí ze dne

11. 12. 2008 (informace dostupné na http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention) a také Nejvyšší soud Kypru v rozhodnutí ze dne 1. 2. 2011 (informace na http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus). Právní úprava implementující citovanou Směrnici o data retention je dle zjištění Ústavního soudu v současné době nadto přezkoumávána i v Polsku či v Maďarsku. Nutnost zajištění co nejpřísnějších záruk a nástrojů k ochraně základních práv jednotlivců při nakládání s jejich osobními údaji z elektronické komunikace zdůraznil i Evropský soudní dvůr ve svém rozhodnutí v řízení o předběžné otázce ze dne 9. 11. 2010 ve spojených věcech *Volker und Markus Schecke GbR GbR* a *Hartmut Eifert v. Land Hessen* (C-92/09 a C-93/09).

53. S ohledem na výše uvedené Ústavní soud konstatuje, že napadená ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a napadenou vyhlášku č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, nelze považovat za ústavně konformní, neboť zřetelně porušují výše vyložené ústavněprávní limity, neboť nesplňují požadavky plynoucí z principu právního státu a jsou v kolizi s požadavky na omezení základního práva na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny, které plynou z principu proporcionality.

54. Nad rámec uvedeného považuje Ústavní soud za nutné zdůraznit, že uvedené nedostatky, které jej vedly k derogaci napadené právní úpravy, nejsou respektovány ani zvláštními právními předpisy, s nimiž napadené ust. § 97 odst. 3 zákona o elektronických komunikacích nepřímo počítá. Zejména pak citované ust. § 88a tr. řádu upravující podmínky použití uchovávaných údajů o uskutečněném telekomunikačním provozu pro účely trestního řízení dle názoru Ústavního soudu výše předestřené ústavněprávní limity a požadavky zdaleka nerespektuje a z toho důvodu se Ústavnímu soudu jeví rovněž protiústavním. Nicméně vzhledem ke skutečnosti, že navrhovateli nebylo v návrhu napadeno, Ústavní soud považuje za nezbytné apelovat na zákonodárce, aby v důsledku derogace napadené právní úpravy zvážil i změnu cit. ust. § 88a tr. řádu tak, aby se stalo ústavně konformním.

VIII. C) Obiter dictum

55. Pouze toliko ve formě *obiter dicta* Ústavní soud konstatuje, že si je samozřejmě vědom skutečnosti, že ruku v ruce s rozvojem moderních informačních technologií a komunikačních prostředků dochází i k výskytu nových a sofistikovanějších způsobů páchání trestné činnosti, kterým je nutné čelit. Nicméně Ústavní soud vyjadřuje pochybnosti nad tím, zda samotný nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů téměř o veškeré elektronické komunikaci je z hlediska intenzity zásahu do soukromé sféry nepřeberného množství účastníků elektronické komunikace nástrojem nezbytným a přiměřeným. Tento názor není v evropském prostoru zdaleka ojedinělým, neboť samotná Směrnice o data retention od samého počátku své existence čelila obrovské vlně kritiky jednak ze strany členských států (např. vlády Irska, Nizozemí, Rakouska či Švédska dlouho otálely či stále ještě vyčkávají s její implementací, přičemž dvě posledně jmenované země tak činí i přes Komisí veřejně avizovanou hrozbu zahájení řízení před Evropským soudním dvorem), jednak ze strany zákonodárců v Evropském parlamentu, Evropského inspektora ochrany údajů (viz závěry z konference k problematice data retention pořádané Komisí dne 3. 12. 2010 v Bruselu, viz http://www.dataretention2010.net/docs.jsp)

či Pracovní skupiny pro ochranu dat zřízené podle čl. 29 Směrnice 95/46/ES (srov. její stanoviska dostupná na http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm), anebo ze strany nevládních organizací (mimo jiné Statewatch, European Digital Rights či Arbeitskreis Vorratsdatenspeicherung - AK Vorrat). Všichni výše uvedení se domáhali buď úplného zrušení předmětné Směrnice o data retention a nahrazení nástroje plošného a preventivního uchovávání provozních a lokalizačních údajů jinými, více přiměřenými nástroji (např. tzv. *data freezing*, jež za splnění stanovených podmínek umožňuje sledování a uchovávání potřebných a vybraných údajů pouze u konkrétního, předem určeného účastníka komunikace), anebo se domáhali její změny, zejména v podobě poskytnutí dostatečných záruk a prostředků ochrany dotčeným jednotlivcům a zpřísnění požadavků na bezpečnost uchovávaných údajů před hrozbou jejich úniků a zneužití ze strany třetích osob.

56. K pochybnostem Ústavní soud dospěl i při zkoumání toho, zda nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů je z pohledu jeho původního účelu (ochrana před bezpečnostními hrozbami a prevence před pácháním zvlášť závažné trestné činnosti) nástrojem efektivním, a to zejména při existenci tzv. anonymních SIM karet, které se vymykají z napadenou právní úpravou předvídaného rozsahu uchovávaných provozních a lokalizačních údajů a které jsou dle vyjádření Policie České republiky až ze 70 % využívány ke komunikaci při páchání trestné činnosti (srov. „*Česká policie chce zakázat anonymní předplacené karty, operátoři se brání*“, iDNES.cz, 18. 3. 2010). V této souvislosti lze odkázat na analýzu Spolkového úřadu vyšetřování SRN (*Bundeskriminalamt*) ze dne 26. 1. 2011, který na základě porovnání statistických údajů o spáchané závažné trestné činnosti na území SRN za období před a po přijetí předmětné právní úpravy k data retention dospěl k závěru, že použití nástroje plošného a preventivního uchovávání provozních a lokalizačních údajů nemělo téměř žádný vliv na snížení počtu spáchaných závažných trestných činů, ani na míru jejich objasňování (samotná analýza a konkrétní statistické údaje jsou dostupné na http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,de/). Obdobné závěry lze přitom učinit i při zběžném pohledu na statistické přehledy kriminality na území České republiky zveřejňované Policií České republiky, např. srovnání statistických údajů za období let 2008 až 2010 (dostupné na http://www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx).

57. V neposlední řadě považuje Ústavní soud za nutné vyjádřit pochybnosti i nad tím, zda je vůbec žádoucí, aby soukromé osoby (poskytovatelé služeb v oblasti internetu a telefonní a mobilní komunikace, zejm. mobilní operátoři a obchodní společnosti zajišťující připojení k internetu), byly nadány oprávněním uchovávat veškeré údaje o jimi poskytované komunikaci, i o zákaznících, jimž jsou jejich služby poskytovány (tzn. údaje jdoucí i nad rozsah údajů, jež jsou dle napadené právní úpravy povinny uchovávat), a volně s nimi za účelem vymáhání pohledávek, rozvoje obchodní činnosti a marketingu disponovaly. Tato skutečnost se Ústavnímu soudu jeví jako nežádoucí zejména z toho důvodu, že v zákoně o elektronických komunikacích ani v jiných právních předpisech není toto oprávnění a jeho účel blíže a podrobněji regulován, nejsou striktně vymezena práva a povinnosti, rozsah uchovávaných údajů, doba a způsob uchovávání, stejně jako nejsou blíže konkretizovány požadavky na jejich zabezpečení a kontrolní mechanismy.

58. S ohledem na výše uvedené proto Ústavní soud rozhodl podle § 70 odst. 1 zákona o Ústavním soudu o zrušení napadených ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a napadené vyhlášky

č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, dnem vyhlášení tohoto nálezu ve Sbírce zákonů (§ 58 odst. 1 zákona o Ústavním soudu).

59. Použitelnost již vyžádaných údajů pro účely trestního řízení bude třeba zkoumat ze strany obecných soudů z hlediska proporcionality zásahu do práva na soukromí v každém jednotlivém individuálním případu. Soudy budou muset především vážit závažnost trestného činu, který měl být naplněn skutkem, pro nějž je vedeno trestní řízení, ve kterém mají být vyžádané údaje využity.

P o u č e n í : ***Proti rozhodnutí Ústavního soudu se nelze odvolat (§ 54 odst. 2 zákona o Ústavním soudu).***

V Brně dne 22. března 2011

Pavel Rychetský
předseda Ústavního soudu