Ústavní soud České republiky

Joštova 8

660 83 Brno 2

*DOPORUČENOU POŠTOU*



V Praze dne 17.3.2010

**Návrh na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů**

**a**

**návrh 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**



**Navrhovatelé:** poslanci Poslanecké sněmovny ČR

| **jméno** | **příjmení** | **rodné číslo** | **bydliště** |
|---|---|---|---|
| Walter | Bartoš | | |
| Marek | Benda | | |
| Petr | Bratský | | |
| Martin | Bursík | | |
| Jan | Bürgermeister | | |
| Jiří | Čepelka | | |
| František | Dědič | | |
| Vladimír | Dlouhý | | |
| Michal | Doktor | | |
| Tomáš | Dub | | |
| Dana | Filipi | | |
| Petr | Gandalovič | | |
| Vladimír | Hink | | |
| Zdeňka | Horníková | | |
| Radim | Chytka | | |
| Kateřina | Jacques | | |
| Miroslav | Jeník | | |
| Jan | Klas | | |
| Jaroslav | Klein | | |
| Jozef | Kochan | | |

| | |
|---|---|
| Petr | Krill |
| Jaroslav | Krupka |
| Ivan | Langer |
| Ondřej | Liška |
| Helena | Mallotová |
| Petr | Nečas |
| Miroslava | Němcová |
| Zbyněk | Novotný |
| Jiří | Papež |
| Alena | Páralová |
| Miloš | Patera |
| Daniel | Petruška |
| Ondřej | Plašil |
| Jiří | Polanský |
| Jiří | Pospíšil |
| Zdeněk | Prosek |
| Přemysl | Rabas |
| Aleš | Rádl |
| Daniel | Reisiegel |
| Daniel | Rovan |
| Jana | Rybínová |
| František | Sivera |
| Pavel | Suchánek |
| Lubomír | Suk |
| Milan | Šmíd |
| Vladimír | Šoltys |
| Jan | Špika |
| Petr | Tluchoř |
| Tomáš | Úlehla |
| Vladislav | Vilímec |
| Tom | Zajíček |

**zastoupeni:** Markem Bendou

**Účastníci řízení:** Parlament České republiky

1. Poslanecká sněmovna
2. Senát

TROJMO

**Přílohy**: 1x plná moc

I.

**Navrhovatel**

Níže podepsaná skupina poslanců Poslanecké sněmovny Parlamentu České republiky využívá tímto svého práva daného ustanovením § 64 odst. 1 písm. b) zákona č. 182/1993 Sb. o Ústavním soudu, ve znění pozdějších předpisů (dále „zákon o Ústavním soudu") a podává návrh na zrušení části zákona a prováděcí vyhlášky dle čl. 87 odst. 1 písm. a) ústavního zákona č. 1/1993 Sb., Ústavy České republiky, ve znění pozdějších předpisů (dále „Ústava").

II.

**Účastník řízení**

Na výše uvedeném ustanovení zákona se usnesl Parlament České republiky, který má tímto postavení účastníka řízení dle § 69 odst. 1 zákona o Ústavním soudu.

III.

**Napadená ustanovení**

Tento návrh směřuje proti ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále „zákon o elektronických komunikacích") a vyhlášce 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 „Vyhláška").

Ustanovení ***§ 97 odst. 3***, jehož zrušení je navrhováno, zní:

*„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. 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).".*

Ustanovení **§ 97 odst. 4**, jehož zrušení je navrhováno, zní:

*„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."*

Zákon o elektronických komunikacích byl vyhlášen ve Sbírce zákonů dne 31. 03. 2005 a nabyl účinnosti dne 01. 05. 2005. Již v předstihu implementoval tehdy jen navrhovanou směrnici, později přijatou jako směrnice Evropského parlamentu a Rady č. 2006/24/ES (dále „Směrnice").

Znění § 97 odst. 3, 4 se od jeho účinnosti změnilo zákonem č. 247/2008 Sb., tímto zákonem byla doplněna definiční ustanovení zákona a došlo k rozšíření požadavků na provozovatele veřejných komunikačních sítí o uchovávání rovněž neúspěšných pokusů o volání (pokud jsou tyto údaje poskytovatelé vytvářejí nebo zpracovávají a zároveň uchovávají nebo zaznamenávají) a dalšímu upřesnění týkajícímu se povinnosti poskytovat údaje příslušným orgánům a stanovení minimální doby k uchovávání těchto údajů na 6 měsíců, maximální 1 rok. V současnosti jsou tyto údaje (s výjimkou údaje o identifikátoru URI nebo jiném identifikátoru služby a jejich parametrech, které jsou **uchovávány** po dobu 3 měsíců) uchovávány v souladu s § 4 Vyhlášky **po dobu 6 měsíců.**

Podrobný popis provozních a lokalizačních údajů, které mají být uchovávány, obsahuje **Vyhláška**. Vzhledem k rozsáhlosti napadené vyhlášky navrhovatelé uvádí příkladný výčet nejdůležitějších údajů, které jsou uchovávány a ve zbytku odkazuje na její znění vyhlášené ve Sbírce zákonů.

U **telefonie** jsou provozovatelé veřejné telefonní sítě zejména povinni shromažďovat údaje :

- o typu uskutečněné komunikace,
- o telefonních číslech volajícího a volaného,
- o datu a času zahájení a ukončení komunikace,
- o čísle IMEI (jde o unikátní číslo přidělené výrobcem mobilního telefonu, které je používáno mimo jiné k blokování přístupu do mobilní sítě v případě nahlášení krádeže telefonu mobilnímu operátorovi),
- o vazbě čísla IMEI s číslem MSISDN (účastnické číslo ve veřejné mobilní telefonní síti),
- o stanicích Start BTS a Stop BTS (díky údajům o stanici BTS lze zjistit polohu mobilního telefonu při uskutečnění telefonického rozhovoru, a to nejen polohu volajícího, ale i volaného, případně polohu mobilního telefonu připojeného k mobilní síti),
- o IP adresách terminálů, kterými bylo zprostředkováno odesílání SMS zpráv sítí Internet,
- o datu a času dobití předplaceného kupónu, o čísle kupónu a o telefonním čísle účastníka.

U **internetu** se jedná zejména o uchovávání údajů:

- o typu připojení, o uživatelském účtu, na základě kterého je určitá osoba připojena k internetu, o datu a času zahájení a ukončení připojení k internetu, o množství přenesených dat (u služeb připojení k síti)
- o identifikaci uživatelského zařízení a účtu, o identifikaci odesílatele, příjemce, o množství přenesených dat (u služeb přístupu ke schránce elektronické pošty a přenosu zpráv elektronické pošty)
- o identifikaci uživatelského zařízení a účtu, o datu a času požadavku na službu, o navštívených internetových stránkách, o vyhledávaných heslech, o množství přenesených dat (u serverových služeb)
- o komunikujících stranách, o datu a času zahájení a ukončení komunikace, o použitých službách a o množství přenesených dat (u dalších služeb elektronických komunikací - zejména u služeb typu chat, usenet, instant messaging a IP telefonie)

**IV.**

**Rozpor s ústavním pořádkem**

Navrhovatel namítá rozpor napadených ustanovení s těmito ustanoveními ústavního pořádku ČR:

a) čl. 7 odst. 1 Listiny základních práv a svobod, vyhlášené usnesením předsednictva České národní rady č. 2/1993 Sb. jako součást ústavního pořádku České republiky (dále jen „Listina"):

*„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."*

b) čl. 10 odst. 2 a 3 Listiny:

*„(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*

*(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě."*

c) čl.13 Listiny:

*„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením."*

d) čl. 8 Úmluvy o ochraně lidských práv a základních svobod (dále „EÚLP"):

*„(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.*

*(2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."*

**V.**

**Podrobné odůvodnění**

Ústavní soud ve své dosavadní judikatuře vychází z toho, že při posuzování souladu zákona s ústavním pořádkem, nelze opomenout hledisko jeho souladu s ratifikovanými a vyhlášenými mezinárodními smlouvami o lidských právech a základních svobodách (viz nález Ústavního soudu sp. zn. Pl. ÚS 36/01), přičemž takovou smlouvu je zejména výše zmíněná EÚLP. Na rozdíl od EÚLP (čl. 8) nestanovuje Listina (čl. 7 odst. 1, čl. 10 odst. 2 a 3, čl. 13) podmínky a meze zásahů do práva na respektování soukromého života a korespondence a odkazuje na úpravu zákonem. V dalším výkladu budou navrhovatelé zejména posuzovat ústavnost napadených ustanovení a jejich soulad s omezeními stanovenými v čl. 8 EÚLP s přihlédnutí k existující judikatuře ESLP, jíž uznává a o niž se opírá i Ústavní soud ve svých rozhodnutích (viz např. nález Ústavního soudu sp. zn. II. ÚS 502/2000) a zejména pak k zásadě proporcionality.

Obsahem napadaných ustanovení je uložení povinnosti fyzickým a právnickým osobám, které zajišťují veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací (tedy především telefonních operátorů a poskytovatelů internetového připojení), 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 (krátké zprávy typu „chat" a telefonie prostřednictvím internetu), specifikované ve vyhlášce získaných při jejich zajišťování a poskytování oprávněným orgánům a to v délce šesti měsíců a následně tyto údaje zlikvidovat.

**Shromažďování údajů o komunikaci jako zásah do soukromého života**

Na základě shora uvedených uchovávaných údajů tak lze sestavit komunikační a pohybový profil jednotlivce odhalující řadu podstatných charakteristik jeho identity a chování.[1].

[1] např. při pokusu prováděném výzkumným centrem při Massachussets Institute of Technology, se ukázalo, že centrum bylo schopno určit s 90% přesností sociální síť pokusných osob, včetně spolupracovníků, známých a přátel. Na základě údajů o pohybu osoby v průběhu 1 měsíce bylo centrum schopno s 95% přesností předpovědět, kdy se bude pokusná osoba nacházet na pracovišti, doma nebo na jiném místě, viz online: http://reality.media.mit.edu/dyads.php.

Dle čl. 8 EÚLP má každý právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Jako zásah do soukromého života a korespondence je podle judikatury ESLP nutné chápat jak kontrolu obsahu pošty a telefonních hovorů (Klass v. Německo), **zjišťování telefonních čísel telefonujících osob** (P. G. a J. H. v. Spojené Království), **tak uchovávání informace, že daná osoba telefonovala s určitou osobou** (Amann v. Švýcarsko). **Není rozhodující**, jak ESLP rovněž judikoval (viz Copland v. Spojené království § 43), zda **shromažďovaná data byla také nějakým způsobem použita.**

Ústavní soud již ve svém nálezu sp. zn. II. ÚS 502/2000 judikoval, že soukromí každého člověka je hodno ochrany ve smyslu čl. 13 Listiny nejen ve vztahu k vlastnímu obsahu zpráv podávaných telefonem, ale i ve **vztahu k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie ve vztahu k údajům o základnových stanicích zajišťujících hovor.** Tyto údaje jsou nedílnou součástí komunikace uskutečněné prostřednictvím telefonu. Totéž logicky platí z povahy komunikace i pro e-mailovou korespondenci a aktivity na internetu.

**Zásahem do základních práv se** nerozumí jen bezprostřední zásah (např. seznámení se s uchovávanými údaji), ale i **taková opatření** státních orgánů, která typicky a předvídatelným způsobem mají za následek **omezení základních práv** či v sobě skrývají značné nebezpečí jejich omezení, **které může kdykoli nastat**[2]. Uchovávání provozních a lokalizačních údajů nelze než považovat za takový zásah, neboť tyto údaje jsou státním orgánům k dispozici a ty si je mohou v budoucnu dle příslušných předpisů vyžádat a využívat zejména na základě § 78 zákona č. 273/2008 Sb., o Policii ČR[3], přičemž policie sama má k těmto údajům přístup dle § 18 zákona o Policii ČR či § 88a trestního řádu a v praxi uplatňuje i na základě § 8 tr.ř. apod.

Uchovávání shora uvedené sady údajů po dobu 6 měsíců 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.

---

[2] Windthorst, Kay: Verfassungsrecht I. Grundlagen, 1. Aufl., München 1994, § 8, odstavec 50 a 52.

[3] § 78 odst. 1 PolZ: „Policie předává zpravodajským službám České republiky, Vojenské policii, ministerstvu, Vězeňské službě České republiky, Celní správě České republiky a dalším orgánům veřejné správy informace včetně informací zpracovávaných v policejních evidencích, které získala při plnění svých úkolů, je-li to nezbytné pro plnění úkolů v rámci jejich působnosti."

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 lidé znali předem okolnosti, kdy stát může výjimečně do jejich soukromého života zasáhnout, a mohli přizpůsobit své jednání tak, aby se tomuto vyhnuli (např. se nepouštěli do bližších kontaktů s pracovníky ambasády nepřátelského státu apod.).[4] Plošný charakter uchovávání provozních a lokalizačních údajů však **možnost reálné volby osob omezuje až vylučuje**.

**Provozní a lokalizační údaje o použití pevné linky, mobilního telefonu, emailu, internetu a o jiném telekomunikačním provozu, jakož i jejich shromažďování, uchovávání a předávání státními orgány tak spadají pod ochranu výše zmíněných článků Listiny a čl. 8 EÚLP.**

## Zásada proporcionality

Dle čl. 8 odst. 2 EÚLP je zásah do soukromí přípustný, pokud je v souladu se zákonem a nezbytný v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Prostor pro uvážení státu, který zde EÚLP dává, není neomezený a podléhá kontrole ESLP. Jeho nejvýznamnější korektiv a omezení představuje princip proporcionality. Omezení, které znamená zásah do práva chráněného EÚLP, musí být vždy **přiměřené vzhledem k významu** daného práva. Ingerence do práva musí být odůvodněna **naléhavou společenskou potřebností a nutností** a přijaté opatření musí být **proporcionální vzhledem ke sledovanému legitimnímu cíli.** Evropský soud ověřuje, zda státní orgán vykonával svou **diskreční pravomoc „v dobré víře, pečlivě a rozumným způsobem"** a zda měl příslušné, dostačující důvody.

ESLP ve věci Klass v. Německo zdůraznil, že pravomoc státních úřadů **tajně sledovat občany je rysem totalitních režimů a z hlediska EÚLP ji lze tolerovat jen v rozsahu, v němž je striktně nezbytná k ochraně demokratických institucí, tedy proporcionálně.** Dále ESLP opakovaně judikoval, že právní předpisy upravující zásah do soukromého života musí s dostatečnou přesností vymezit rozsah diskreční pravomoci svěřené příslušným orgánům a způsob, jakým má být tato pravomoc vykonávána s ohledem na legitimní cíl daného opatření tak, aby byla občanům zajištěna dostatečná ochrana proti zvůli. Je třeba zkoumat, zda je zásah přiměřený legitimnímu cíli, tedy zda je v rovnováze zájem společnosti (na omezení práva) k zájmu jednotlivce (na jeho dodržení).[5]

---

4 viz Kruslin v. Francie, Huvig v. Francie

5 Rotaru v. Rumunsko §§ 55art, Amann v. Švýcarsko §§ 76 a 80, Khan v. Spojené Království § 26, Valenzuela Contreras v. Španělsko §§ 60 a 61, Kopp v. Švýcarsko §§ 72 a 75, Funke v. Francie § 57, Niemietz v. Německo § 37, Malone v. Spojené Království §§ 79 a 80 ad.

Jak judikoval Ústavní soud (viz nález Ústavního soudu sp. zn. II. ÚS 502/2000), tak zásada proporcionality se vztahuje i na zásahy státu do práva na soukromí upraveného v čl. 13 Listiny: *„...Jestliže ústavní pořádek České republiky připouští průlom této ochrany (práva na ochranu soukromí podle čl. 13 Listiny), děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a na tom, aby takové činy byly zjištěny a potrestány. Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany státní moci, jestliže jde o zásah nezbytný ve výše uvedeném smyslu. K tomu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování..."*

Omezení základních práv je tedy přípustné jen tehdy, pokud je k dosažení zamýšleného účelu vhodné a nezbytné a s tím spojený zásah není dle své intenzity v nepoměru k významu věci a újmě, kterou způsobí dotčeným osobám.

Přiměřenost daného opatření je tedy především nutné hodnotit:

1. z hlediska **závažnosti a rozsahu zásahu** do základních práv, v tomto případě práva na soukromí
2. z hlediska **legitimity cíle**, k jehož dosažení má omezení základních práv sloužit, a **přínosu těchto zásahů** k jeho dosažení
3. z hlediska **nebezpečí, která jsou spojena s uplatňováním daných opatření** a z hlediska **nebezpečí zneužití** uchovávaných údajů.

**Ad 1) Závažnost a rozsah zásahu do práva na soukromí**

Závažnost a rozsah zásahu je třeba posuzovat podle toho, za jakých předpokladů je zásah přípustný, kolik a kteří nositelé základních práv jím budou dotčeni a jak intenzivně. Intenzita zásahu odvisí v oblasti informací mezi jiným od **druhu, rozsahu a myslitelného použití uchovávaných údajů.** Při zjišťování možností použití shromážděných údajů je třeba též zohlednit, **jaké negativní důsledky** na základě přijatých opatření nositelům základních práv hrozí nebo jichž se mohou odůvodněně obávat. Dále je důležité posoudit **využitelnost a použitelnost údajů**, a to zejména s ohledem na skutečnost, že získané údaje mohou být kombinovány s dalšími daty, čímž mohou být získávány kvalitativně hodnotnější informace.

Při posouzení závažnosti zásahu do práva na soukromí je nutné především do jaké míry je možná identifikace nebo zachování anonymity dotčené osoby s ohledem na uchovávaná data. Vzhledem k tomu, že údaje mají sloužit hlavně ke trestnímu stíhání a odvracení nebezpečí, nelze anonymitu údajů předpokládat. Policie ČR má právo v souladu s § 97 odst. 5 zákona o elektronických komunikacích žádat informace o účastnících veřejně dostupné telefonní služby. Tyto údaje lze pak

například prostřednictvím telefonního čísla propojit s provozními a lokačními údaji. Anonymní tak mohou zůstat pouze ty údaje, u nichž nebude možné provést toto propojení.

Zavedení povinnosti uchovávat provozní a lokalizační údaje představuje citelný zásah do soukromí dotčených osob, poněvadž tyto údaje otevírají široké možnosti jejich použití a zkombinování s dalšími údaji, což může mít velmi silné neblahé důsledky pro dotčené osoby. Tato všeobecná povinnost k uchovávání provozních a lokalizačních údajů vede k tomu, že nekontrolovaná a nemonitorovaná telekomunikace je téměř vyloučena, což je nutno považovat za obzvlášť intenzivní zásah do svobody soukromí a korespondence.

Často se uvádí, že uchovávání tolika provozních a lokalizačních údajů nepředstavuje tak závažný zásah do základních práv a svobod jako případné uchovávání obsahu telekomunikace. Správnost tohoto tvrzení však nelze posuzovat pouze podle druhu shromažďovaných údajů, ale i z hlediska jejich užitečnosti a jejich možného použití. To souvisí jednak s účelem jejich shromažďování a dále s možnostmi jejich zpracování a propojení s dalšími údaji. V konkrétním případě tak může být zásah do soukromí závažnější v případě uchovávání a využívání provozních a lokalizačních údajů než v případě samého obsahu komunikace. Jako příklad lze uvést obsahově nikoli důležitý telefonát mezi dvěma osobami, který však může mít daleko větší vypovídací hodnotu o soukromí osoby z hlediska místa, data, doby uskutečnění telefonátu a identifikace hovořících osob, než z hlediska obsahu samotného hovoru.

Dále je třeba zohlednit možnosti zpracování a propojení jednotlivých údajů. V současné době je automatické zpracování obsahu např. telefonických hovorů těžko realizovatelné; ke zpracování a vyhodnocení je zapotřebí lidského činitele. Naproti tomu ukládání, třídění a vyhodnocení provozních a lokalizačních údajů a jejich spojování s dalšími informacemi lze provádět automaticky s pomocí vyhledávače, což zvyšuje riziko zneužití a závažnost dopadu zpracování těchto údajů do soukromí konkrétního jednotlivce.

Nadto se v oblasti internetu **rozlišování mezi obsahovými daty a provozními a lokalizačními údaji stírá**, neboť znalost provozních údajů (URL = „internetová adresa" či „webová stránka") umožňuje zjistit i obsah komunikace zadáním URL do stavového řádku internetového prohlížeče (tj. **z údaje o navštívené internetové stránce lze zjistit i její obsah).**

**Z výše uvedeného je patrné, že vypovídací hodnota provozních a lokalizačních údajů může být s vypovídací hodnotou obsahu telekomunikace minimálně srovnatelná, někdy ji může i převyšovat. Lze tak dovodit, že provozní a lokalizační údaje je třeba chránit stejně jako údaje o obsahu komunikace.** Závažnost zásahu do práva na ochranu soukromí a korespondence lze

posoudit jen na základě konkrétních okolností v konkrétním případě. Rozdíly v právní úpravě mezi obsahovými údaji a provozními a lokalizačními údaji ohledně přípustnosti zásahu do práva na ochranu soukromí a korespondence jsou tak neodůvodněné.

Pro posouzení zásady proporcionality jsou primárně rozhodující právně přípustné možnosti použití. Je však nutno zkoumat i ostatní, reálně a technicky existující možnosti použití; a to též z důvodu, že rozšíření okruhu státních zásahů (rozšíření přístupu do již vytvořené databáze pro další subjekty) je v porovnání s nově zavedenou možností státního zásahu a dohledu nad provozními a lokačními údaji (vytvoření databáze a přístupu do ní) vždy podstatně snazší. Za další je nutné počítat s rizikem nezákonného použití a zneužití uchovávaných dat, zejména v situaci, kdy je zneužití jen těžko zjistitelné.

Uchovávané údaje umožňují **odhalení kontaktů** účastníků telekomunikačního provozu a sítě **jejich vztahů jak soukromého tak profesního rázu.** Navíc je možné, což se týká zejména mobilní telefonie, na jejich základě **zjistit místa pobytu a pohybu** účastníků telefonie. Uchovávání internetových dat ve spojení s přístupovým protokolem umožňuje **vystopovat navštívené internetové stránky a mapovat chování** jednotlivců na internetu. Je tedy nutné zdůraznit, že z uchovávaných informací, **lze dovodit celou řadu dalších (v řadě případů velmi citlivých) údajů** o dané osobě. V řadě případů lze z identity adresáta telefonátu nebo e-mailu odhalit citlivý údaj o odesilateli (např. pokud je adresátem lékař-specialista), podobně lze z navštívených internetových stránek zjišťovat data o názorovém smýšlení, zdravotním stavu nebo sexuální orientaci dané osoby. Velké množství dat 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 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.** Dokladem je závěr studie výzkumného centra při Massachussets Institute of Technology, které zaznamenávalo údaje z mobilních telefonů pokusného vzorku osob, které svým rozsahem odpovídají rozsahu údajů, které je podle výše zmíněného ustanovení zákona o elektronických komunikacích povinen shromažďovat provozovatel sítě elektronických komunikací (shromažďovány byly údaje o poloze telefonu, užívání mobilního telefonu a o proběhlé komunikaci). Z takto získaných dat bylo možné s velmi vysokou přesností (nad 90%) odvodit a dokonce předvídat pohyb sledovaných osob, pozici sledované osoby v sociální síti, jakož i vzorce chování jednotlivců i celého systému (kde se jedinec pohybuje, kde se bude pohybovat, s kým a kde se bude stýkat apod.)[6]

6 Eagle, Nathan; Pentland, Alex Sandy: Eigenbehaviors: identifying structure in routine, In. Behavioral Ecology & Sociobiology; May2009, Vol. 63 Issue 7, p1057-1066, http://reality.media.mit.edu/pdfs/eigenbehaviors.pdf

V současnosti celá řada společností (i2, Visual Analytics, Memex, Orion Scientific, Pacific Northwest National Labs und Genesis EW) nabízí programy, které umožňují získávání informací ze sestaveného komunikačního profilu.[7] Analýza telekomunikačních dat je nejlevnějším a nejběžnějším způsobem, jak získat obrovské množství informací o soukromém, profesním a veřejném životě dané osoby.[8]

Co se týče okruhu osob dotčených uchovávaním provozních a lokalizačních údajů, lze uvést, že jsou **dotčeny všechny osoby, které používají jakýkoli telekomunikační prostředek (telefonie, užívání služeb internetu).** Telekomunikační zařízení se dnes již nevyužívají pouze ke komunikaci mezi lidmi, ale zasahují do širokého spektra každodenních činností. S ohledem na současný vývoj společnosti a rozmach mobilních telefonů a internetu je tak prakticky zasažen každý. Podle údajů Českého statistického úřadu vlastnilo v roce 2008 cca 87,9% obyvatel ČR nad 16 let mobilní telefon, v posledních třech měsících použilo internet 54% obyvatel ČR.[9] V roce 2007 byly v ČR připojeny celkem 2 403 000 pevných telefonních linek.[10]

Zvláště je nutné upozornit na fakt, že dochází **i k ukládání provozních a lokalizačních údajů o komunikaci osob, které jsou vázány povinností mlčenlivosti.** Povinnost mlčenlivosti je tímto způsobem dotčena. Týká se to jak advokátů tak např. poradců (po telefonu, anonymní poradny pro alkoholiky, manželské poradny, poradny pro HIV pozitivní, těhotenské poradny, krizové linky, atd.), lékařů a psychoterapeutů nebo novinářů (právo na ochranu zdroje). Uchovávání a možné využívání provozních a lokalizačních údajů o jejich telekomunikaci je přímo limituje ve výkonu jejich povolání.

V napadených ustanoveních nejsou stanoveny žádné předpoklady, na základě nichž mají být údaje uchovávány. Naopak, údaje jsou uchovávány **bez existence konkrétního podezření**. Optikou napadených ustanovení je tak ve skutečnosti každá osoba považována za podezřelou bez existence konkrétních okolností, které by k tomuto podezření opravňovaly, což je v právním státě nepřípustné. Zásahy do základních práv s ohledem na obecné zájmy mohou být legitimní, nikoli však ve všech případech. Jinak by byla **přípustná obecná kontrola** a dohled nad občany státu a základní práva by tak ztratila na významu, což **by odporovalo principům svobodného právního státu.**

Právo jednotlivce na svobodu si žádá, aby pro zásah do jeho práv **existovala určitá dostatečná spojitost, blízkost mezi daným nebezpečím a zásahem směřujícím k jeho odstranění.** Dostatečná blízkost je zásadně dána tehdy, pokud osoba na základě konkrétních okolností v jednotlivém případě je podezřelá, že ohrozila chráněné hodnoty. Obecné domněnky a zkušenosti

---

7 Wikipedia, Traffic Analysis, http://en.wikipedia.org/wiki/Traffic_analysis

8 Welp, Jürgen: Die TKÜV im System staatlicher Abhörbefugnisse, S. 3-14 in: Holznagel, Bernd / Nelles, Ursula / Sokol, Bettina (Hrsg.): Die neue TKÜV (TelekommunikationsÜberwachungsverordnung), 1. Aufl., München 2002, 3 (9)

9 http://www.czso.cz/csu/2008edicniplan.nsf/p/9701-08

10 http://www.czso.cz/csu/redakce.nsf/i/pevna_telefonni_sit

k odůvodnění takového podezření nestačí. Ohledně uchovávaných údajů, které zásadním způsobem zasahují do práva na ochranu soukromí a korespondence a umožňují bez větší námahy sestavit komunikační a pohybový profil jednotlivce, taková **spojitost a blízkost dána není.**

**Ad 2) Legitimita cíle a přínos zásahů do základních práv k jeho dosažení**

Dle čl. 1 odst. 1 Směrnice byla **Směrnice vydána za účelem** harmonizace povinností poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, pokud jde o uchovávání některých údajů jimi vytvořených nebo zpracovaných, s cílem zajistit dostupnost těchto údajů pro účely **vyšetřování, odhalování a stíhání závažných trestných činů,** které jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech. Z důvodové zprávy vlády k ustanovení § 97 zákona o elektronických komunikacích vyplývá, že účelem ustanovení § 97 je čelit zvyšujícím se rizikům při zabezpečení bezpečnosti a obrany České republiky, přičemž bližší odůvodnění chybí.

Je nutné poznamenat, že podle čl. 8 odst. 2 EÚLP je zásah do soukromí přípustný ve vztahu k boji s kriminalitou **pouze tehdy, pokud slouží k předcházení zločinnosti**. Lze konstatovat, že preventivní, všeobecné uchovávání telekomunikačních údajů bez existence konkrétního důvodu míří hlavně do minulosti a může tak sloužit hlavně k objasňování již spáchaných trestných činů. Stíhání již spáchaných trestných činů může mít preventivní účinky jen do té míry, že pachateli trestného činu bude v páchání dalších činů zamezeno uložením trestu odnětí svobody nebo v důsledku trestního řízení může být odškodněna oběť trestného činu. **Zásah do soukromí za účelem objasnění již spáchaného trestného činu je dle navrhovatelů v rozporu s čl. 8 EÚLP.**

Dle názoru navrhovatelů lze očekávat, že uchovávání dat může pomoci k naplnění stanovených cílů spíše málo a v méně významných případech a nelze očekávat dlouhodobý a pozitivní vliv na snížení kriminality a zvýšení bezpečnosti v souvislosti s používáním telekomunikačních prostředků. V oblasti boje proti organizovanému zločinu a terorismu, vůči nimž je Směrnice hlavně namířena, lze očekávat velmi nízký efekt vzhledem k možnostem použití anonymních komunikačních sítí, zejména ze třetích států, kde povinnost k identifikaci při používání telekomunikačních služeb neexistuje, dále například předplacených telefonních služeb, které jsou anonymní (lze zjistit pouze telefonní číslo osoby, ale už ne její adresné osobní údaje), internetových kaváren, anonymizace prostřednictvím proxy serverů (využití prostředníka mezi klientem a cílovým počítačem, vůči němuž vystupuje sám jako klient), systému The Onion Router (umožňuje šifrovaný přenos dat prostřednictvím sítě routerů, kde je odesílatel nedohledatelný) apod.

**Zásah do soukromí se tak paradoxně může více týkat osob, které se na závažné trestné činnosti nepodílejí, než osob, které ji páchají a mají zvýšený zájem svoji komunikaci provádět anonymně. Napadená ustanovení tak v konečném důsledku nevedou k účinnějšímu boji proti závažné trestné činnosti, ale pouze k využívání jiných forem komunikace mezi osobami, proti jejichž trestné činnosti jsou namířeny.** Předkladatelé právní úpravy ani věcně příslušný ústřední

resort státní správy nedodali informace, v kolika a v jakých případech před zavedením této úpravy, která se sebou nese obrovské kvantitativní navýšení uchovávaných dat 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 je **neprokázané, zda zavedení úpravy o povinnosti uchovávat všechny údaje o telefonické a elektronické komunikaci povede (nebo již vedlo) ve srovnání s předcházející úpravou skutečně ke zlepšení vyšetřování, odhalování a stíhání závažných trestných činů a odvracení hrozeb, zvýšení procenta objasněnosti trestných činů, 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.

Příslušné statistiky o využívání provozních a lokalizačních údajů v České republice nemají navrhovatelé k dispozici a nechávají na úvaze Ústavního soudu, zda si je vyžádá od příslušných orgánů (budou-li je mít tyto k dispozici). Z následující tabulky, která odráží vývoj kriminality v ČR, vyplývá, že množství zjištěných i objasněných trestných činů zůstává více méně stejné v době před zavedením i v době po zavedení napadených ustanovení a v procentuálním srovnání objasněnost trestných činů od počátku platnosti napadených ustanovení dokonce klesá.

Tab. 1: Počet zjištěných a objasněných trestných činů v ČR

| | počet zjištěných trestných činů celkem | počet objasněných trestných činů | počet objasněných trestných činů v % |
|---|---|---|---|
| 2004 | 351 529 | 134 444 | 38,20% |
| 2005 | 344 060 | 135 281 | 39,30% |
| 2006 | 336 446 | 133 695 | 39,70% |
| 2007 | 357 391 | 138 852 | 38,90% |
| 2008 | 343 799 | 127 906 | 37,20% |

Zdroj: Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2008, Praha 2009, Tab. 1, s. 73

**Ad 3) Nebezpečí chybného vyhodnocení a zneužití uchovávaných údajů**

Vyhodnocování údajů o telekomunikačním provozu s sebou přináší nebezpečí jejich chybné interpretace a obvinění nevinného člověka. V této souvislosti je vhodné připomenout některé případy, kdy policie tyto údaje vyhodnotila nesprávně. V Rakousku byl nigerijský občan držen neoprávněně několik měsíců ve vazbě, protože na základě rozboru jeho telefonních kontaktů byl v podezření, že je vůdcem gangu prodejců drog. Následně se ukázalo, že je pouze vyhledávaný poradcem v černošské komunitě ve Vídni. Ve Švédsku byly v souvislosti s počítačovou kriminalitou zatčeni nevinní lidé, protože skuteční pachatelé zneužili jejich přístupové kódy. V Německu byl vyšetřován muž proto, že vstupoval neoprávněně na placené erotické stránky, aniž by za toto platil. Muž se bránil, že tyto stránky nikdy nenavštívil. Dalším šetřením bylo zjištěno, že pachatelem je někdo jiný, kdo neoprávněně využíval jeho bezdrátovou „wifi" síť. V souvislosti s posledním jmenovaným případem je nutné připomenout fakt, že jak v případě telefonních hovorů, tak v případě pohybu na internetu nelze s absolutní jistotou určit, jaká osoba tímto způsobem komunikuje. Vzniká tak nebezpečí záměny osoby, která komunikaci skutečně prováděla s osobou, která např. uzavřela smlouvu s telefonním operátorem nebo s poskytovatelem internetu. **Vypovídací hodnota těchto údajů se v tomto světle jeví slabou vzhledem k deklarovanému cíli právní úpravy.**

Vedle nebezpečí špatné interpretace získaných údajů o telekomunikačním provozu je zde široká možnost zneužití těchto údajů. Podle vyjádření Evropského inspektora ochrany údajů lze rozlišit tyjí nebezpečí zneužití uchovávaných údajů [12]:

1. samotnými poskytovateli
2. orgány činnými v trestním řízení
3. zpravodajskými službami

Oprávnění Policie ČR žádat od poskytovatelů poskytnutí provozních a lokalizačních údajů o telekomunikačním provozu dává § 66 odst. 3 zákona č. 273/2008 Sb., o Policii České republiky. Poskytovatel by podle tohoto ustanovení měl umožnit Policii ČR k těmto údajům dálkový a nepřetržitý přístup.

Podle § 78 odst. 1 téhož zákona *„Policie předává zpravodajským službám České republiky, Vojenské policii, ministerstvu, Vězeňské službě České republiky, Celní správě České republiky a dalším orgánům veřejné správy informace včetně informací zpracovávaných v policejních evidencích, které získala při plnění svých úkolů, je-li to nezbytné pro plnění úkolů v rámci jejich působnosti."* Veškeré údaje o telekomunikačním provozu **se tak mohou dostat prostřednictvím Policie ČR**

11 Verfassungsbeschwerde Vorratsdatenspeicherung z 31. 12. 2007, str. 86,
http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf

**k zpravodajským službám, jejichž kontrola činnosti je omezená.** Ochrana utajovaných skutečností (s nimiž zpravodajské služby často pracují) uvnitř kontrolních orgánů není z důvodu vysokého počtu členů příslušných parlamentních komisí dostatečná. Tendencí zpravodajských služeb je pak nesdělovat kontrolním orgánům utajované skutečnosti, což je vedeno obavou z prozrazení probíhajících operací, prozrazení svých zaměstnanců nebo zpravodajských zdrojů a v důsledku toho i z možného ohrožení jejich bezpečnosti. Kontrola zpravodajských služeb je tedy v České republice spíše formální.[13] Nedostatečná kontrola vytváří prostor k utajení neschválených operací, k možnému zneužití zpravodajských služeb nebo k porušování lidských práv a svobod. V této souvislosti je nutné připomenout, že **kontrolu samotné Policie ČR nelze považovat za nezávislou**, protože její inspekce i po provedených změnách nadále zůstala organizační součástí Ministerstva vnitra.

Nedostatečná kontrola využívání provozních a lokalizačních údajů je posílena tím, že orgánům oprávněným k využívání těchto údajů nebyla zároveň uložena povinnost informovat osobu, jejíž údaje byly vyžádány, ačkoli v případě srovnatelných odposlechů a záznamů telekomunikačního provozu je tato povinnost informovat uložena (§ 88 odst. 8 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů).

**Nebezpečí zneužití provozních a lokalizačních údajů lze spatřovat zejména v rozšiřování účelů, k nimž budou údaje využívány. Toto nebezpečí je obzvláště velké za stávajícího stavu, kdy nejsou podrobně vymezeny podmínky, za kterých může dojít k využívání** výše zmíněných údajů. Tato úprava tak nahrává extenzivnímu využívání příslušných databází, jak co se týče množství údajů, které z nich budou čerpány, tak co týče množství subjektů, které k tomuto budou oprávněny.

Rovněž lze očekávat další prohlubování zásahů státu do základních práv občanů. Zákonné úpravy schválené v evropských zemích na základě Směrnice lze považovat za první krok. V této souvislosti je nutné zmínit některé legislativní návrhy v evropských zemích. Již schválená novela švédského telekomunikačního zákona nařizuje všem švédským operátorům a internetovým poskytovatelům zasílat kopie každé komunikace (včetně jejího obsahu) přímo švédské zpravodajské službě, která je může využívat bez jakéhokoli soudního povolení.[14] Britská vláda zase prosazuje národní úpravu, která počítá se soustředěním všech údajů o položkově rozepsaných telefonních účtech, záznamech o mobilní telefonii a logů o internetovém provozu v jedné centrální vládní databázi.[15]

---

12 Stanovisko Evropského inspektoru ochrany údajů 2005/C 298/1, § 32

13 Zetocha, K.: Parlamentní kontrola zpravodajských služeb, podkladový materiál v rámci projektu Institutu pro evropskou politiku EUROPEUM „Příspěvek k debatě o reformě zpravodajských služeb v České republice: Pracovní panel k reformní agendě", 2008, str. 4, http://www.europeum.org/doc/pdf/Karel_Zetocha_skupina11.pdf

14 ENDitorial: Sweden is listening to all internet and phone, EDRi, 2. 7. 2008, http://www.edri.org/edrigram/number6.13/sweden-fra-adoption

15 UK Government will store all phone, Internet traffic data, EDRi, 21. 5. 2008, http://www.edri.org/edrigram/number6.10/uic-isp-traffic-data

Ze strany poskytovatelů hrozí zejména zneužívání údajů o svých klientech k marketingovým účelům. Provozní a lokalizační údaje poskytovatelé zpracovávali částečně již dříve například za účelem provedení vyúčtování. Museli však podle § 6 odst. 1 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů zpracovávat osobní údaje pouze po dobu, která byla nezbytná k naplnění stanovených účelů. Tato doba byla zpravidla podstatně kratší než je doba 6 měsíců, která je minimální dobou pro uchovávání těchto údajů podle § 97 odst. 3 zákona o elektronických komunikacích.

Velmi reálné je nebezpečí zneužití provozních a lokalizačních údajů třetími osobami. Osobami, které mohou tyto osobní údaje zneužít, jsou velmi často zaměstnanci společností nebo státních orgánů, které údaje zpracovávají, ale i dalšími osobami (např. hackery). Toto zneužití může mít řadu podob. Osobní údaje mohou být například prodány dalším subjektům. Zaměstnanec společnosti AOL ve Spojených státech prodal v roce 2004 k marketingovým účelům osobní údaje o 92 milionech zákazníků této společnosti za 152 000 dolarů.[16] Dalším důvodem tohoto zneužití může být průmyslová špionáž, ale i ovlivňování politiky. Zájem zločineckých struktur o komunikaci významných politiků a podnikatelů dokazují dva rozsáhlé případy neoprávněných odposlechů mobilních telefonů těchto osob v Řecku a v Itálii.[17]

Je skutečností obecně známou, že v České republice několikrát unikly policejní odposlechy, které byly následně zveřejněny v médiích (např. odposlechy funkcionářů fotbalových klubů, kauza Kořistka, odposlechy v souvislosti s vyšetřováním tzv. Berdychova gangu, odposlechy Františka Mrázka atd.)[18] Obsahy některých těchto odposlechů byly zveřejněny ještě předtím, než byl někdo obviněn, tedy ve fázi vyšetřování, kdy by měl mít ke spisu přístup pouze policejní orgán, případně státní zástupce a soudce. S největší pravděpodobností se tedy zneužití své pravomoci dopustili někteří ze zaměstnanců Policie ČR. Ministr vnitra Langer v listopadu 2007 uvedl, že dosud v žádném případě zveřejnění odposlechů telekomunikačního provozu nebyl zjištěn viník tohoto úniku informací.[19] **Podle výsledků šetření Úřadu pro ochranu osobních údajů z roku 2006 ve věci zabezpečení osobních údajů Policií ČR bylo zjištěno, že „k osobním údajům vypovídajícím o probíhajícím trestním řízení má od počátku přístup velký počet osob, a to u Policie České republiky a u jiných subjektů.** Např. u jednoho datového souboru bylo evidováno 4 305 aktuálně používaných uživatelských oprávnění, k dalšímu 33 300 uživatelských oprávnění v samotné Policii České republiky. Údaje o probíhajícím trestním řízení zpracovávané v určitých elektronických datových souborech Policie ČR byly podle ÚOOÚ dále zpřístupňovány pro samoobslužné vyhledávání nepřetržitým dálkovým přístupem, na

16 AOL-Mitarbeiter wegen Verkaufs von Kundendaten verhaftet, Heise Verlag, 24.06.2004, http://www.heise.de/newsticker/AOL-Mitarbeiter-wegen-Verkaufs-von-Kundendaten-verhaftet-Update-/meldung/48542

17 Abhörskandal entsetzt die Griechen, Handelsblatt, 02.02.2006, http://www.handelsblatt.com/news/-Default.aspx?_p=200051&_t=ft&_b=1028595; Der ganz, ganz große Lauschangriff, Spiegel Online, 21.09.2006, http://-www.spiegel.de/panorama/justiz/0,1518,438499,00.html

18 Vantuch, P.: Zveřejňování odposlechů v médiích, Právní rádce, 28. 5. 2008, http://pravniradce.ihned.cz/c4-10078260-25053060-700000_d-zverejnovani-odposlechu-v-mediich

základě písemného požadavku nebo telefonicky jiným správcům: třem ministerstvům, zpravodajským službám a Národnímu bezpečnostnímu úřadu." [20] Je zřejmé, že stejně jako opakovaně dochází k únikům policejních odposlechů, tak lze i očekávat úniky provozních a lokalizačních údajů ze strany Policie ČR. V této věci přitom nehraje roli fakt, zda Policie ČR vede databázi těchto údajů sama, nebo pokud ji, jako v případě ČR, vedou poskytovatelé a Policie ČR má k této databázi nepřetržitý a dálkový přístup.

Další nebezpečí zneužití osobních údajů je např. zneužití hackery. Známé německé sdružení hackerů Chaos Computer Club opakovaně upozorňuje na nebezpečí plynoucí z uchovávání a využívání provozních a lokalizačních údajů. Ve své zprávě vypracované na vyžádání Spolkového ústavního soudu k této otázce podrobně rozebírá jak to, jakými způsoby lze tato data využívat, tak rovněž nebezpečí úniků (tématika technického zabezpečení sítí poskytovatelů, tzv. backdoor virů, slouží k proniknutí proniknutí a následnému ovládání počítače, problematika zabezpečení údajů u malých poskytovatelů internetu apod.)[21]

Zabezpečení osobních údajů je všude v Evropě problematické a úniky těchto údajů jsou velmi časté. Dle společnosti Ponemon Institute, které provedla výzkum v 785 britských společnostech zaměřených na informační technologie, přiznalo celých 55 % těchto společností ztrátu dat, 49 % zaznamenalo více než dva případy během dvou posledních let.[22] V České republice rovněž dochází k celé řadě úniků osobních údajů včetně úniků dat o klientech finančních institucí (Uniqa, ČSOB atd.)[23], které by měly tyto údaje obzvláště důkladně zabezpečit. **Při velkém množství společností, které zajišťují telekomunikaci (zejména v případě internetu), nelze očekávat odpovídající zajištění těchto provozních a lokalizačních údajů. V konečném důsledku nejefektivnější ochranou proti možným zneužitím uchovávaných údajů by bylo žádné takové údaje neuchovávat** a nevystavovat tak zároveň občany pocitům neustálého sledování a kontroly, jaké shromažďování a uchovávání provozních a lokalizačních údajů dle napadených ustanovení představuje.

---

19 Koukal, J.: Úniky informací: všichni bijí na poplach, ale nic nedělají, Právo, 19. 11. 2007, http://www.novinky.cz/domaci/127088-uniky-informaci-vsichni-biji-na-poplach-ale-nic-nedelaji.html

20 ÚOOÚ: Zveřejňování a zabezpečení osobních údajů Policií ČR při jejich zpracování v rámci probíhajícího trestního řízení, http://www.uoou.cz/uoou.aspx?menu=0&submenu=10&loc=483

21 Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung, 9. 6. 2009, http://www.ccc.de/vds/VDSfinal18.pdf

22 Alarmující výzkum: Více než polovině britských firem již unikla data, Security World, 17. 10. 2008, http://securityworld.cz/securityworld/alarmujici-vyzkum-vice-nez-polovine-britskych-firem-jiz-unikla-data-251

23 ČSOB zjistila únik dat, banka podala trestní oznámení, iHned, 10. 12. 2007, http://ekonomika.ihned.cz/c1-22587250-csob-zjistila-unik-dat-banka-podala-trestni-oznameni; Za únik dat tisíců klientů může hacker, říká pojišťovna UNIQA, iDnes, 3. 9. 2009, http://ekonomika.idnes.cz/za-unik-dat-tisicu-klientu-muze-hacker-rika-pojistovna-uniqa-p5f-/ekoakcie.asp?c=A090903_163321_ekonomika_fih;

**Shrnutí**

V oblasti telekomunikačních technologií se stále ve větší míře lidé setkávají, předávají si informace, vytvářejí různé zájmové skupiny apod. V této oblasti se tedy realizují jejich základní práva a svobody jako např. právo jednotlivce na informační sebeurčení, svoboda projevu, náboženského vyznání, bádání, petiční právo, právo sdružovací ad. Tato základní práva mohou být v budoucnu zpracováváním provozních a lokalizačních údajů významně ohrožena, zejména pokud bude docházet k zneužívání a únikům těchto údajů.

Dle navrhovatelů jsou **cíle a pravděpodobný a očekávatelný užitek vyplývající z povinnosti uchovávání provozních a lokalizačních údajů ve srovnání s tím spojeným zásahem do základních práv dotčených osob v hrubém nepoměru.** Jak bylo uvedeno v odůvodnění návrhu, tak využívání provozních a lokalizačních údajů umožňuje získání obrovského množství informací o soukromí osob a zároveň umožňuje s velkou pravděpodobností určit pohyb a činnost těchto osob v budoucnu.

Naopak, **naplnění stanoveného cíle** „vyšetřování, odhalování a stíhání závažných trestných činů" tak jak je definován v čl 1 odst. 1 Směrnice lze, vzhledem k možnostem anonymizace komunikace, považovat za problematické a zvolený prostředek (tedy plošné preventivní uchovávání provozních a lokalizačních údajů) **za málo efektivní.** Napadená ustanovení dopadnou především na osoby, které se nedopouštějí žádné trestné činnosti, protože osoby, které se jí dopouštějí, budou svoji komunikaci anonymizovat. Podle názoru navrhovatelů byla napadená ustanovení přijata v rozporu se zásadou proporcionality, která představuje nejvýznamnější korektiv státních zásahů do práva na soukromí.

Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu je tedy z výše zmíněných důvodů **v rozporu s čl. 7 odst. 1, čl 10 odst. 2 a 3 a čl. 13 Listiny, jakož i čl. 8 EÚLP.**

**VI.**

**Předběžná otázka vůči Evropskému soudnímu dvoru**

Navrhovatelé uváději, že ačkoliv je napadená právní úprava úpravou vnitrostátní, na kterou je třeba vztáhnout kritéria vyplývající z ústavního pořádku ČR, jedná se současně o problematiku, jejíž původ pramení z komunitárního práva, konkrétně pak z transpozice Směrnice do vnitrostátního právního řádu České republiky.

Navrhovatelé uváději, že existuje **významné riziko, že samotná Směrnice je neplatná z hlediska práva ES, a to z důvodu jejího rozporu se základními právy Společenství**, resp. s právem na ochranu rodinného a soukromého života, které ESD považuje za potřebné dodržovat a chránit. ESD přitom v otázce základních práv **vychází ze znění EÚLP** a jejího výkladu Evropským soudem pro lidská práva – viz rozsudek ESD z 20.05.2003, spojené věci C-465/00, C-138/01 a C-139/01, sbírka rozhodnutí 2003, str. I-04989, odst. 68 an.

Ústavní soud však není kompetentní k tomu, aby posuzoval otázky platnosti norem komunitárního práva, když takové otázky spadají do výlučné pravomoci ESD. Proto navrhovatelé dávají Ústavnímu soudu na zvážení **předložení předběžné otázky (ne)platnosti Směrnice k posouzení přímo ESD, a to v souladu s čl. 234 Smlouvy ES**. Navrhovatelé jsou názoru, že Ústavní soud lze považovat za soudní orgán, který je podle čl. 234 Smlouvy ES povolán k podávání předběžných otázek. Ačkoli obecně platí, že vznesení předběžné otázky není nutné, pokud se danou otázkou *„zabývala předchozí ustálená judikatura ESD, bez ohledu na povahu řízení, která vedla k těmto rozhodnutím, a dokonce i tehdy, pokud daná otázka nebyla identická"*. Jinak řečeno, jde o situaci, kdy předcházející rozhodnutí ESD již pojednala o právní otázce řešené v daném případě (*CILFIT odst. 14*).

O neplatnosti Směrnice již rozhodoval ESD, avšak rozsudek Soudního dvora ze dne 10.2.2009 ve věci C-301/66 o žalobě na neplatnost Směrnice č. 2006/24/ES podané Irskem, se **týkal pouze volby právního základu Směrnice, nikoli porušení základních práv.** V odůvodnění ESD výslovně uvádí, cit.: *„Je rovněž třeba upřesnit, že žaloba podaná Irskem se týká pouze volby právního základu, a nikoli případného porušení základních práv vyplývajícího ze zásahů do výkonu práva na soukromí, které s sebou směrnice 2006/24 přináší."*[24]

Rozhodnutí ESD o případné (ne)platnosti Směrnice z důvodu jejího namítaného rozporu se základními právy je pro předmětné řízení o abstraktní kontrole norem **nezbytné. Posouzení této otázky je zásadního významu pro Ústavní soud při posuzování ústavní konformity** napadeného transpozičního ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích, jakož i napadené Vyhlášky, když Ústavní soud při abstraktní kontrole norem přihlíží k případné komunitárněprávní dimenzi napadených zákonných ustanovení.

## VII.

## Ústavní přezkum v zemích EU

Navrhovatelé by rádi upozornili Ústavní soud na probíhající ústavní přezkum obsahově totožných ustanovení jako jsou napadená, která implementovala Směrnici v některých evropských zemích. Navrhovatelé zejména upozorňují na přezkum příslušných ustanovení telekomunikačního zákona **německým Spolkovým ústavním soudem** (řízení je **vedeno pod sp. zn. 1BvR 256/08**). Tento **soud prodloužil předběžným omezením omezení účinnosti zákona na případy, kdy dojde k ohrožení života, zdraví nebo svobody osoby, ohrožení existence nebo bezpečnosti státu nebo pokud je nutné tyto údaje použít k odvrácení obecného nebezpečí. Využití bylo vázáno na povolení nezávislého soudu.**[25]

---

[24] Rozsudek ESD ze dne 10.2.2009, C-301/66, odst. 57.
25 Rozhodnutí: http://www.bundesverfassungsgericht.de/entscheidungen/rs20081028_1bvr025608.html

K otázce souladu těchto ustanovení zákona nařizujících preventivní plošné uchovávání dat o komunikaci celé populace se vyslovil mj. též správní soud ve Wiesbadenu. Ten vyhodnotil plošné uchovávání dat týkající se emailů, telefonických hovorů a používání Internetu celé populace jako nepřiměřené. V rozhodnutí (rozhodnutí ze dne 27. 02. 2009 číslo 6 K 1045/08. WI) se uvádí: "soud je toho názoru, že uchovávání dat porušuje základní právo na ochranu soukromí. V demokratické společnosti není takového opatření zapotřebí. I ti, kdo se ničím neprovinili, se mohou cítit ohroženi rizikem zneužití a pocitem, že je nad nimi vykonáván dohled [...]. (Směrnice) nerespektuje princip proporcionality garantovaný Článkem 8 ECHR, a proto je neplatná."[26]

**Meritorní rozhodnutí Spolkového ústavního soudu bylo vyneseno dne 2. 3. 2010.** Spolkový ústavní soud pozastavil příslušnou právní úpravu účinnou od počátku roku 2008 a nařídil okamžitou likvidaci všech osobních údajů zpracovávaných na základě této právní úpravy. Soud rovněž přednesl požadavky na budoucí právní úpravu. Především se jedná o stanovení velmi přísných pravidel pro uchovávání a používání získaných údajů, data by měla být šifrována a celý proces by měl podléhat transparentní kontrole. Vedle bezpečnostních opatření soud stanovil i omezení pro uchovávání údajů na 6 měsíců a omezení využívání údajů. Přístup k nim by měl být umožněn například pouze u závažných trestných činů. Lidé by měli být napříště rovněž informováni, pokud si státní orgány vyžádají jejich údaje, tajné využívání dat by mělo být možné pouze v individuálních případech a se svolením soudu.[27]

Soudnímu přezkumu byla příslušná ustanovení podrobena i v dalších zemích. Na konci roku 2008 zrušil bulharský ústavní soud čl. 5 bulharského zákona o elektronických komunikacích, kterým se implementovala Směrnice.[28] V říjnu 2009 zrušil příslušný zákon, který implementuje Směrnici rumunský ústavní soud. [29] Ústavní přezkum příslušných ustanovení byl zahájen také v Maďarsku.[30]

## VIII.

### Existence podmínky pro přezkum ústavnosti transpozičního ustanovení

Navrhovatelé uvádějí, že **Směrnice, ve své současně platné podobě, představuje výkon pravomocí orgánů ES způsobem, který ohrožuje samotnou podstatu materiálního právního státu.** Z dosavadní judikatury Ústavního soudu vyplývá, že, *„pokud by vývoj v ES, resp. EU, ohrožoval samotnou podstatu státní svrchovanosti ČR nebo podstatné náležitosti demokratického právního státu, bylo by třeba trvat na tom, aby se těchto pravomocí opětovně ujaly vnitrostátní orgány ČR,*

26 Rozhodnutí: http://wiki.vorratsdatenspeicherung.de/Urteil_VG_Wiesbaden_2009-02;

27 Rozhodnutí: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html

28 Bulgarian Court annuls a vague article of the data retention law, EDRi, 17. 12. 2008, http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

29 http://www.edri.org/edrigram/number7.20/romania-data-retention-law-unconstitutional

*přitom platí, že k ochraně ústavnosti je povolán Ústavní soud (čl. 83 Ústavy ČR).*"[31] V takovém případě je **Ústavní soud povolán k posouzení vnitrostátní transpoziční právní úpravy, tj. k posouzení napadených ustanovení, z hlediska souladu s ústavním pořádkem České republiky.**

Podle jiného nálezu Ústavního soudu může Ústavní soud *„zkoumat, zda některý akt orgánů Unie nevybočil z pravomocí, které Česká republika podle čl. 10a Ústavy na Evropskou unii přenesla. Ústavní soud však předpokládá, že taková situace může nastat jen v případech zcela výjimečných; za ty by bylo možné považovat zejména opuštění hodnotové identity a již uvedené překročení rozsahu svěřených kompetencí."*[32]

**Konkrétně pak navrhovatelé uvádějí, že napadená ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích a napadená Vyhláška, jakožto transpoziční úprava, představují neproporcionální zásah do základních práv uvedených v Listině základních práv a svobod, a to takový, který lze navíc považovat za porušující podstatné náležitosti demokratického právního státu.** Jedná se zejména o zásah do základního práva na soukromí uvedeného v čl. 7 odst. 1 Listiny, čl. 10 odst. 2 a 3 Listiny.

V řadě dosavadních rozhodnutí již Ústavní soud nastínil obsah pojmu podstatných náležitostí demokratického právního státu, např. ve svém nálezu ze dne 10. 9. 2009 ve věci vedené pod sp. zn. Pl. ÚS 27/09. V tomto nálezu pak Ústavní soud uvádí, že již ve svém rozhodnutí ve věci vedené pod sp. zn. Pl. ÚS 19/93 Ústavní soud odkázal na stanoviska doktrinální, dle nichž k podstatným náležitostem demokratického právního státu ve smyslu čl. 9 odst. 2 a 3 Ústavy patří *„především svrchovanost lidu a principy obsažené v čl. 5 a 6 Ústavy a* ***přirozenoprávní ustanovení Listiny základních práv a svobod,*** *která zakládají ústavní právo na odpor (čl. 23 Listiny)", resp. vyjádřeno jinak, jsou tyto náležitosti „koncentrovány v několika článcích I. hlavy Ústavy a I. a V. hlavy Listiny a slavnostně prohlášeny v Preambuli Ústavy".*

Mezi **podstatné náležitosti demokratického právního státu tak bezpochyby patří též zásada uvedená v hlavě I. Listiny, čl. 4 odst. 4, a to zásada proporcionality**, která se vztahuje na zákonná omezení základních práv a svobod, dle které *„(4) Při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena."*

Napadená ustanovení, jakož i Směrnice, dle navrhovatelů představují zásah do uvedených základních práv, který není v souladu s čl. 4 Listiny a který lze proto považovat za ohrožení podstatných náležitostí demokratického právního státu.

---

30 Hungarian Data Retention Law - challenged at the Constitutional Court, EDRi, 4. 6. 2008, http://www.edri.org/edrigram/number6.11/hungary-data-retention-constitutional

[31] Nález Ústavního soudu ze dne 8/3/2006, sp. zn. Pl. 50/04.
[32] Nález Ústavního soudu ze dne 23/11/2008, sp. zn. Pl. 19/08

V nálezu ze dne 1. 3. 2007 sp. zn. Pl. ÚS 8/06 Ústavní soud konstatoval, že v případech střetů základních práv či svobod s veřejným zájmem, resp. 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 (přiměřenosti v širším smyslu), jež může být také nazývána zákazem nadměrnosti zásahů do práv a svobod. Tato obecná zásada zahrnuje tři kritéria posuzování přípustnosti zásahu. Prvním z nich je princip způsobilosti naplnění účelu (nebo také vhodnosti), dle něhož musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku. Dále se pak jedná o princip potřebnosti, dle něhož je povoleno použití pouze nejšetrnějšího - ve vztahu k dotčeným základním právům a svobodám - z více možných prostředků. Třetím principem je princip přiměřenosti (v užším smyslu), dle kterého újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních."*

Pro posouzení dané věci je rovněž relevantní, že **princip proporcionality též vyplývá z ustálené judikatury ESD**. Ústavní soud již konstatoval, že *„nelze ústavněprávní přezkum otázek týkající se [oblasti komunitárního práva] ... provádět zcela izolované, bez ohledu na kritéria a meze regulace stanovené komunitárním právem a v minulosti dotvořené judikaturou ESD."*[33] *Tyto „principy komunitárního práva vyjádřené v dosavadní judikatuře ESD Ústavní soud nechává prozařovat do výkladu ústavního práva"*[34]. Judikatura ESD uvádí, že ačkoli mohou být základní práva při provádění komunitárních politik předmětem určitého omezení, příslušné omezení nesmí být neproporcionální vůči účelu, kterým je obecný zájem sledovaný Společenstvím: *„Základní práva uznaná ESD nejsou absolutní, ale musejí být posuzována z hlediska své sociální funkce. V důsledku toho lze akceptovat omezení výkonu těchto práv, zejména v souvislosti se společnou organizací trhu, a to za předpokladu, že tato omezení korespondují s účelem, jímž je obecný zájem sledovaný Společenstvím, a nezakládají s ohledem na tento účel neproporcionální a neakceptovatelný zásah porušující samotnou podstatu těchto práv."*[35]

Ústavní soud dále ve své dosavadní judikatuře vychází z toho, že při posuzování souladu zákona s ústavním pořádkem rovněž nelze opomenout hledisko jeho **souladu s ratifikovanými a vyhlášenými mezinárodními smlouvami o lidských právech a základních svobodách (viz nález Ústavního soudu sp. zn. Pl. ÚS 36/01), přičemž takovou smlouvu je zejména výše zmíněná EÚLP**. Stejně tak i ESD v otázce základních práv zpravidla vychází ze znění EÚLP a jejího výkladu ESLP. Navrhovatelé proto uvádějí, že pro výklad předmětných ustanovení Listiny je též relevantní výklad a aplikační praxe ustanovení čl. 8 EÚLP, které definuje základní právo na respektování

[33] Nález Ústavního soudu ze dne 8/3/2006, sp. zn. Pl. 50/04.
[34] Nález Ústavního soudu ze dne 8/3/2006, sp. zn. Pl. 50/04.

soukromého a rodinného života. Článek 8 EÚLP stanoví, cit.: *„(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. (2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."*

## IX.

## Návrh

**1. Na základě výše uvedených skutečností navrhovatelé navrhují, aby plénum Ústavního soudu vydalo podle ustanovení § 70 odst. 1 zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů, nález, kterým se § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 186/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb. a zákona č. 281/2009 Sb., zrušuje.**

**2. Na základě výše uvedených skutečností navrhovatelé dále navrhují, aby plénum Ústavního soudu vydalo podle ustanovení § 70 odst. 1 zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů, nález, kterým se 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, zrušuje.**

skupina poslanců

## VIII.

## Přílohy

**Plné moci**

---

[35] Např. Rozsudek ESD *č.5/88 - Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft [1989] ECR2609, odst. 18.*