

**UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA**

DIPLOMOVÁ PRÁCE

Data retention – ukládání provozních a lokalizačních údajů

Autor: Lukáš Jirovský

Vedoucí práce: Mgr. František Korbel, PhD.

Poděkování

Chtěl bych poděkovat vedoucímu práce, Mgr. Františkovi Korbelovi, PhD., za cenné rady při psaní práce.

Také bych chtěl poděkovat za postřehy z praxe odborníkům z telekomunikací, konkrétně JUDr. Michalu Krejčíkovi ze společnosti O2 a Mgr. Alici Selby, Mgr. Miroslavovi Uříčařovi, JUDr. Kláře Novotné, PhD. a Mgr. Patricii Šedivé ze společnosti T-Mobile.

Čestné prohlášení

Prohlašuji, že jsem tuto diplomovou práci na téma Data retention vypracoval samostatně za použití literatury a zdrojů v ní uvedených. Dále prohlašuji, že práce nebyla dříve publikována, nebyla vcelku ani částečně obhájena jako práce diplomová či bakalářská.

V Praze dne

.....

Lukáš Jirovský

Obsah

1	Úvod do předmětu práce.....	8
2	Co je data retention?	9
2.1	Úvod.....	9
2.2	Rozdíly data retention oproti odposlechům	10
2.3	Předpisy	10
2.4	Pojmy provozní a lokalizační údaje	10
2.5	Provozní a lokalizační údaje v praxi.....	11
2.6	Co data retention není?	14
3	Právo na soukromí.....	16
3.1	Vývoj práva na soukromí v ČR.....	16
3.2	Právo na soukromí v ústavním pořádku a mezinárodních smlouvách..	17
3.3	Obsah práv	18
3.3.1	Právo na soukromí.....	18
3.4	Související judikatura.....	20
3.4.1	Malone vs. Spojené království (1984).....	20
3.4.2	ÚS ČR – použitelnost zpravodajského odposlechu v trestním řízení.....	20
4	Zákonná úprava a judikatura	22
4.1	Provozní údaje v období před směrnicemi a vstupem do EU.....	22
4.1.1	Zákon o telekomunikacích	22
4.1.2	ÚS – Právo na ochranu zpráv podávaných telefonem.....	22
4.1.3	Novela trestního řádu	23
4.2	Evropské směrnice do roku 2006	23
4.3	Zákon o elektronických komunikacích – první verze	24
4.3.1	Popis.....	24
4.3.2	Zákonodárny proces	25
4.3.3	Provozní údaje a lokalizační údaje a prováděcí vyhláška	26
4.3.4	Policie a další oprávněné subjekty	27
4.4	Směrnice 2006/24/ES	28
4.4.1	Důvody pro přijetí směrnice.....	28
4.4.2	Obsah směrnice	29
4.4.3	Odpor proti směrnici 2006/24/ES.....	30
4.5	Novela zákona v roce 2008	31

4.6	Rozsudek SD EÚ z února 2009	31
4.7	Rozhodnutí Spolkového ústavního soudu v roce 2010	32
4.8	Nález Ústavního soudu ČR z roku 2011	33
4.8.1	Soukromí	34
4.8.2	Přípustnost zásahů	35
4.8.3	Názor ÚS na právní úpravu	35
4.8.4	Rozhodnutí	36
4.8.5	Obiter dictum.....	36
4.8.6	Druhý nález Ústavního soudu	37
4.9	Novela ZoEK v roce 2012.....	38
4.10	Stanovisko generálního advokáta Soudního dvoru EU	41
4.10.1	Proporcionalita směrnice	43
4.10.2	Omezení výkonu práv dle čl. 52 Listiny práv Evropské unie	44
4.10.3	Závěr stanoviska.....	45
4.11	Zrušení směrnice č. 2006/24/ES.....	45
4.12	Vývoj v ČR po zrušení směrnice č. 2006/24/ES.....	47
4.13	Rozhodnutí po zrušení směrnice č. 2006/24/ES v dalších zemích EU	47
4.13.1	Kde bylo data retention zrušeno	48
4.13.2	Kde data retention zůstává v platnosti.....	49
4.14	Další úprava související s data retention	50
4.14.1	Evidence počtu případů.....	50
4.14.2	Čísla tísňového volání	50
4.14.3	Pátrání po osobách.....	50
4.14.4	Zákon o kybernetické bezpečnosti	51
5	Data retention v praxi.....	52
5.1	Rozsah ukládaných dat	52
5.1.1	Pevná telefonní síť (hovory).....	52
5.1.2	Mobilní telefonní síť (hovory)	52
5.1.3	Datová síť (připojení k Internetu)	52
5.1.4	Provozní data v pevné telefonní síti – hlas.....	53
5.1.5	Provozní a lokalizační data v mobilní síti – hlas	54
5.1.6	Internet	55
5.1.7	Sítě elektronických komunikací s přepojováním paketů.....	57
5.2	Postup při vydávání dat	61
5.3	Náklady.....	62

5.4	Problémy na straně soudů.....	62
5.5	Poskytování shromážděných údajů zákazníkům.....	63
5.5.1	Osobní údaje vs. provozní údaje	63
5.5.2	Konkrétní případy (SRN a ČR).....	63
5.5.3	T-Mobile Czech Republic a. s.....	65
5.5.4	O2 Czech Republic a. s.	65
5.5.5	Vodafone Czech Republic a. s.	65
5.6	Poskytování údajů kvůli vyúčtování služeb.....	66
5.7	Čestnost předávání dat státním orgánům	69
5.7.1	Počty vyžádání dat	69
5.7.2	Počty úkonů.....	70
5.7.3	Druh komunikace (poskytnutá data)	71
5.7.4	Stáří poskytnutých dat.....	72
5.8	Statistiky trestné činnosti.....	73
5.8.1	Typy trestné činnosti (zjištěné trestné činy).....	74
5.8.2	Typy trestné činnosti (objasněné trestné činy)	75
5.8.3	Vývoj objasněnosti trestných činů dle typu	76
5.8.4	Největší změny v objasněnosti trestných činů po nálezů ÚS	77
5.9	Shrnutí pro rok 2013	83
6	Závěr	84
7	Seznam použitých zdrojů	85
7.1	Seznam použitých právních zdrojů.....	85
7.2	Seznam použité judikatury	88
7.3	Seznam dalších zdrojů.....	89
8	Seznam zkratk	94
9	Anotace	95
10	Abstract.....	95
11	Seznam obrázků	96
12	Seznam tabulek	96
13	Seznam příloh.....	97
14	Přílohy.....	98
14.1	Vyjádření O2 k poskytování provozních dat pro účely vyúčtování.....	98

15	Klíčová slova.....	100
16	Keywords	100

1 Úvod do předmětu práce

Spolu s rozvojem moderních způsobů komunikace vzniká velké množství informací, které podrobně popisují každodenní životy občanů – ať už jde o to, kam jsme volali, jaké internetové stránky jsme navštívili nebo i například, kde jsme se pohybovali před několika měsíci. Z toho důvodu jde o cenné zdroje informací při vyšetřování trestné činnosti. Souhrnně se tato problematika označuje data retention.¹

Cílem této práce je popsat, v jakých případech mluvíme o data retention, jakých údajů konkrétně se týká, jaké subjekty si je mohou vyžádat a za jakých okolností. Práce také popisuje historii a důvod ukládání těchto dat, vývoj právní úpravy a také otázky, které toto téma vzbuzuje z důvodu možného narušování soukromí jednotlivců. Cílem je také odpovědět na otázku přípustnosti takovýchto zásahů do soukromí osob a otázku zvýšení objasňenosti trestných činů při použití provozních a lokalizačních dat.

Česká právní úprava této otázky prošla (a stále prochází) rozsáhlým vývojem – od prvních žádostí policie o poskytnutí dat koncem devadesátých let přes rozsáhlou povinnost stanovenou zákony, rozhodující nálezy Ústavního soudu a novou, přesněji vymezenou úpravu.

Na úrovni Evropské unie je situace podobná – Soudní dvůr Evropské unie rozhodující směrnici v dubnu 2014 zrušil a nyní záleží na jednotlivých členských státech, jak je problematika upravena.²

Práce se také věnuje otázce poskytování těchto dat jednotlivcům, tedy osobám, o nichž byla posbírána – tedy z pohledu ochrany osobních údajů.

Součástí práce je také porovnání statistik o objasňenosti trestné činnosti v dobách, kdy bylo data retention v českém zákoně pozastaveno a srovnání se situací, kdy standardně funguje.

¹ Retention = zachycení

² Šlo o směrnici č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí z 15. března 2006

2 Co je data retention?

2.1 Úvod

Pod názvem **data retention** se označuje **ukládání provozních a lokalizačních údajů** u poskytovatelů telekomunikačních služeb (tzn. převážně operátorů telekomunikačních sítí a poskytovatelů připojení k internetu – přesněji vymezeno jde o provozovatele služeb elektronických komunikací dle zákona č. 127/2005 Sb. o elektronických komunikacích (ZoEK)).

Tyto údaje jsou poskytovateli standardně ukládány i bez zákonné povinnosti, zejména pro vyúčtování služeb, diagnostiky sítě či marketingové účely. Jde o primární důvod jejich ukládání – až později začalo docházet k jejich využití pro odhalování trestné činnosti. Zákonná úprava řeší nejen **poskytování informací státu** (typicky Policii ČR), ale také dobu jejich ukládání, rozsah a vůbec možnosti operátorů, jak je **mohou sami využívat**. Mluvíme-li tedy o zákonné úpravě ukládání provozních dat, nejde vždy jen o „špehování občanů“, jak popisují odpůrci data retention. Jde také o ochranu listovního tajemství (zachování důvěrnosti zpráv), tedy také ochranu zákazníků před případným zneužitím zjištěných informací ze strany operátorů.

Problematika poskytování provozních dat policii (a dalším subjektům) je příbuzná odposlechům (hlavně z pohledu zásahu do soukromí a povinností poskytovatelů), od odposlechů se však data retention odlišuje – ať už fakticky či zákonnou úpravou.³

³ Pojem „policie“ je v tomto případě použit jako zjednodušení, protože dle data retention mohou být data poskytována i dalším subjektům – Bezpečnostní informační službě, České národní bance a Vojenskému zpravodajství – policie však tvoří subjekt nejčastější. Podrobnější informace o oprávněných subjektech lze nalézt v kapitole 4.3.4 této práce.

Jde o problematiku poměrně novou, která stále prochází významnými změnami, a to jak na vnitrostátní, tak evropské úrovni. První české judikáty, které předcházely zákonné úpravě, pocházejí z roku 2000.

2.2 Rozdíly data retention oproti odposlechům

Zatímco po nařízení odposlechu se ukládá i samotný obsah hovoru či telekomunikačního provozu, problematika data retention řeší ukládání údajů o provozu bez znalosti jejich obsahu.⁴ Z tohoto důvodu odposlech představuje větší zásah do soukromí, ovšem až na základě zákonného důvodu a schválení soudem.

Data retention však sleduje všechny občany „preventivně“, ale bez ukládání obsahu komunikace – oprávněný státní orgán má přístup pouze k údajům o daném účastníkovi, jehož provozní data si vyžádá a to i zpětně – nejdéle za období posledních šesti měsíců.

2.3 Předpisy

Problematika data retention je upravena jak směrnicemi EU, tak českými normami. Kromě ZoEK a prováděcích vyhlášek zde má významnou úlohu zákon č. 141/1961 Sb. (trestní řád – *TrŘ*) a zákon č. 273/2008 Sb., o policii. Vzhledem k tomu, že otázka právní úpravy je poměrně obsáhlá (o data retention rozhodoval i Ústavní soud), pojednává o ni kapitola číslo 3.

2.4 Pojmy provozní a lokalizační údaje

Provozní údaje jsou dle § 90 ZoEK definovány jako jakýkoliv údaj zpracováváný pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.

⁴ Soudem dle § 88 Trestního řádu pro zvlášť závažný úmyslný trestný čin a nebo věcech BIS nebo Vojenského obranného zpravodajství

Lokalizačními údaji se pak dle § 91 tohoto zákona rozumí jakékoli údaje zpracované v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.

2.5 Provozní a lokalizační údaje v praxi

Počátkem devadesátých let byla v ČR k dispozici pouze pevná telefonní síť, která používala analogové vytáčení – bylo-li nutné zjistit údaje například o volajícím čísle, bylo potřeba tak učinit během konání hovoru. Jakmile jedna ze stran zavěsila, všechna spojení v ústřednách a dalších síťových prvcích po cestě se rozpojila a zpětně nebylo možné již tyto údaje zjistit.⁵ Samotné účtování pak probíhalo pomocí sčítání tzv. impulzů na mechanickém počítadle – dnes bychom to přirovnali spíše k odečítání vody či měřiči ujetých kilometrů ve starších autech.

Koncem devadesátých let a počátkem 21. století došlo k výraznému rozvoji telekomunikací, díky kterému také vzniklo data retention.

V červnu roku 2002 byl dokončen proces digitalizace pevné telekomunikační sítě Českého Telecomu, který přinesl zákazníkům nové služby. Díky digitálním ústřednám tak bylo jednoznačně jasné odkud-kam probíhá hovor a od impulzů došlo k přechodu na modernější systém tzv. CDR.⁶

Již koncem devadesátých let také vznikaly první mobilní sítě postavené na systému GSM, který se používá dodnes.⁷ Síť GSM pokryly prakticky celou republiku

⁵ Z toho důvodu je možné v nespočtu detektivních románů a filmů vidět scény, ve kterých bylo nutné potenciálního pachatele „držet na lince“ alespoň určitou dobu, aby bylo možné zjistit, odkud volá.

⁶ Call Detail Record – technické soubory obsahující informace pro účtování. Standardně jde o typ jeden hovor = jeden řádek v souboru s informacemi o zdroji, cíli, ceně/tarifu apod.

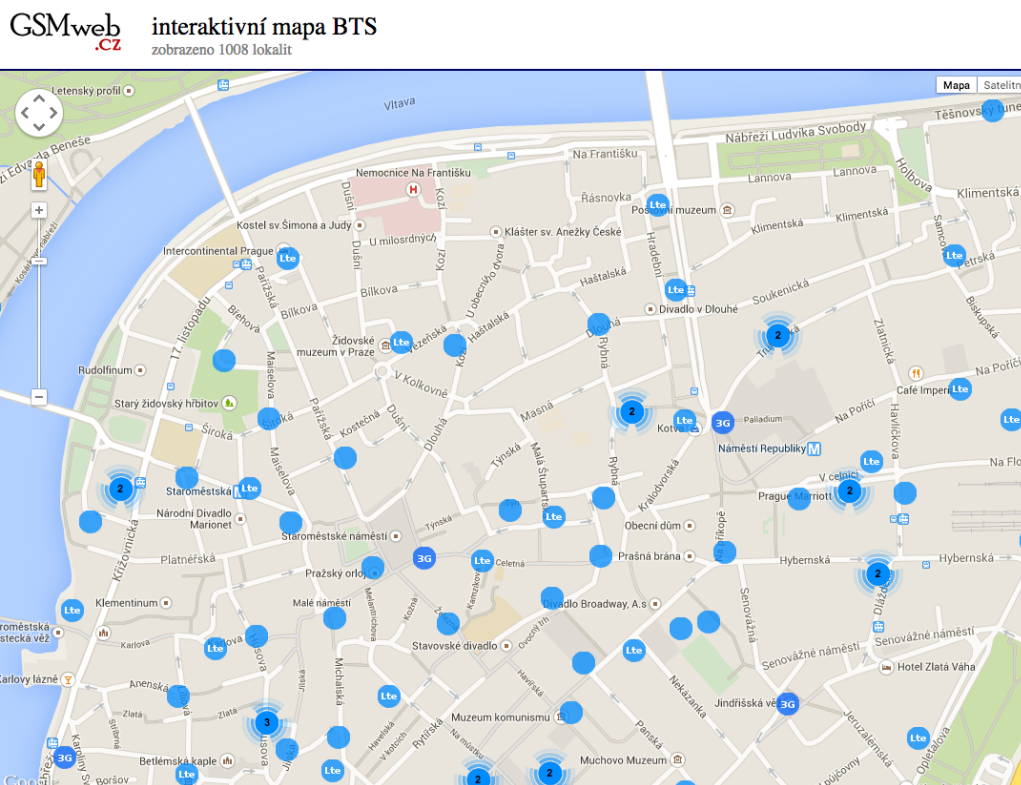
⁷ Pro zájemce o více informací doporučuji přednášku Jiřího Peterky: Historie a současný stav české mobilní telefonie z 12. 11. 2014, dostupná online: <http://www.earchiv.cz/papers/p70/slide.php3?l=1&me=1>

(i Evropu) základnovými stanicemi (tzv. BTS), mezi kterými se uživatel pohybuje.⁸ Díky tomu také začalo mít smysl hovořit o lokalizačních údajích – u pevné sítě ví operátor přesně, kde se volající nachází (kam je zavedena pevná linka) – ať už z důvodu účtování služeb (kam poslat fakturu), tak fyzického propojení sítě pro směrování hovoru. U mobilní sítě se zákazník pohybuje – síť tak musí vědět, do jaké buňky (na úrovni BTS) hovor spojit. Ačkoliv GSM umožňuje vzdálenost mezi základnovou stanicí a telefonem až 35 km, v praxi je síť samozřejmě mnohem hustší – z důvodu pokrytí (členitost terénu) a také samozřejmě kapacity – jedna stanice zvládne obsloužit maximálně osm hovorů zároveň.⁹ Ve městech se tak přesnost pohybuje kolem stovek metrů. Pro představu – počty BTS se v ČR pohybují kolem 6-7 tisíc na jednoho operátora.

⁸ BTS = Base Transceiver station, základnová stanice mobilní sítě

⁹ Nebo přesněji řečeno „zvládala“ v prvním systému GSM. S rozvojem dalších typů sítí (jako např. LTE) už probíhá plánování na základě jiných parametrů. Jde však o názornou ukázkou, proč jsou dnešní sítě tak husté.

Obrázek 1: Příklad mapy BTS jednoho z operátorů v centru Prahy



Zdroj: Mapa BTS T-Mobile dle GSMweb.cz [online]
dostupné z <http://www.gsmweb.cz>, cit. 2014-10-02

Důležité však je, že nejde o údaj, který by se použil pouze v případě hovoru (či jiného spojení). Síť musí mít přehled o mobilních zařízeních neustále, protože pouze základnová stanice, ve které je přístroj přihlášen, na něj posílá např. údaj o přichozím hovoru.¹⁰ Spolu s tím vzniká velmi přesný obraz toho, kde a v jakých časech se zákazníci pohybují.¹¹

Kromě rozvoje telefonní sítě (pevné i mobilní) došlo v tomto období ještě k další zásadní změně, která se týká data retention – rozšíření připojení k internetu.

¹⁰ Tzv. paging

¹¹ Příkladem, kde se tyto parametry využívají, jsou například tzv. LBS – Location Based Services. Služby, které jsou využívány pro posílání informací na zákazníky v dané oblasti. Může jít o reklamu nebo například informaci o pohřešovaném dítěti.

Původní vytáčené připojení k internetu (tzv. dial-up v pevné síti, CSD/HSCSD vytáčené hovory v mobilní síti) se postupně vyvinulo v trvalé připojení i u nefiremních zákazníků. V případě pevných sítí pomocí technologie xDSL (a CATV u rozvodů kabelové televize), v případě mobilní sítě pomocí GPRS a obdobných technologií.¹²

Velké množství technických dat o provozu přináší také samotný internet. Například síťové prvky jsou schopné uchovávat informace, která data jimi protékla (odkud a kam), webové servery poskytující stránky si často ukládají, jakému návštěvníkovi poskytly jaký soubor apod.¹³

Vidíme tedy, že díky tomuto ohromnému rozmachu telekomunikací extrémně narostlo množství technických informací, které vznikají o chování zákazníků – ať už v případě tradičních hovorů, tak připojení k internetu nebo informací o jejich fyzickém pohybu.

Konkrétní údaje, které je operátor povinen státnímu orgánu poskytnout, jsou rozebrány v kapitole číslo 5 – jde o informace stanovené prováděcí vyhláškou.

2.6 Co data retention není?

V prostředí internetu mluvíme o data retention jen u poskytovatelů připojení, zákon se netýká provozovatelů webových služeb. Ti jsou provozovateli služeb informační společnosti, kterým zákon tyto povinnosti neukládá. Neznamená to, že by se policie nemohla dostat k takovým datům, nejde však o režim spadající do ZoEK, který se týká poskytovatelů telekomunikačních služeb.¹⁴

¹² Konkrétně EDGE, UMTS, HSPA, LTE, LTE-A – jde o označení mobilní sítě (či technického řešení pro přenos dat), pojmy uvedeny dle postupného vývoje těchto technologií.

¹³ Část, která už nepatří poskytovateli připojení.

¹⁴ Například pro poskytnutí záznamů od inzertního serveru pro účely vyšetřování podvodů.

Stejně tak v případě lokalizačních údajů nejde o systémy určování polohy, jakými jsou GPS či Galileo. V případě GPS jde o jednostranný systém, kdy zařízení, které určuje polohu, jen přijímá data od satelitů a nic nevysílá – není tedy technická možnost, jak tato data zjistit.¹⁵ U Galilea je obousměrná komunikace v plánu, nicméně systém teprve vzniká a také žádná legislativa týkající se data retention zatím s využitím takovýchto dat nepočítá.

Velmi omezeně se data retention dotýká hromadného zpracovávání dat pro statistické účely (tzv. *big data*). V těchto případech jsou schopni operátoři dodat např. údaje o tom, jak často se uživatelé vrací na určité místo, odkud tam jezdí, jak dlouho na daném místě setrvávají apod. Při zpracování těchto údajů je vždy důsledně dbáno na anonymizaci dat – nejde tedy o sledování konkrétních osob (telefonních čísel), jak je pro data retention typické. Jde například o projekt operátora T-Mobile, KMPG a Národního parku Šumava poskytující statistiky o návštěvnosti parku.¹⁶

Provozní údaje (resp. údaje odpovídající svým obsahem provozním údajům dle ZoEK) mohou být ukládány i jinými subjekty – například výrobcem operačního systému telefonu. Společnost Google, autor systému Android, ve svých Zásadách ochrany soukromí, zmiňuje možnost automaticky shromažďovat: „*informace z protokolu telefonování, jako je vaše telefonní číslo, číslo volajícího, čísla přeměrování, čas a datum hovorů, trvání hovorů, údaje o směrování zpráv SMS a typy hovorů*“.¹⁷ Ani toto ukládání dat nepatří pod problematiku data retention (ZoEK), ale pod ochranu osobních údajů (spolu s instituty jako souhlas se zpracováním apod.).

¹⁵ U zařízení používajícího pouze GPS modul, nikoliv služby, které například údaj o aktuální poloze posílají po mobilní síti.

¹⁶ Pro zájemce o více informací doporučuji článek Mobilenet.cz, Big Data ze sítě T-Mobile pomáhají na Šumavě (uveden ve zdrojích).

¹⁷ Zásady ochrany soukromí společnosti Google [online] [cit. 2014-12-02] Dostupné z <http://www.google.com/intl/cs/policies/privacy/>

3 Právo na soukromí

Ukládání provozních dat se samozřejmě výrazně střetává s právem na soukromí jednotlivců.

3.1 Vývoj práva na soukromí v ČR

První kodifikace práva na soukromí se objevila v zákoně č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního, který tvořil součást Ústavy 1920 – šlo však jen o ochranu listovního tajemství.

Zákon č. 141/1950 Sb., občanský zákoník, úpravu práva na soukromí neobsahoval (pouze § 22 týkající se ochrany jména).

Zákon č. 40/1964 Sb., občanský zákoník (ve znění novelizace zákonem č. 509/1991 Sb.), upravoval ochranu soukromí, jména a projevů osobní povahy fyzické osoby (§ 11) a dále nutnosti svolení pořízení nebo použití písemností osobní povahy.

Zákon č. 89/2012 Sb., občanský zákoník (*NOZ*) upravuje ochranu soukromí v § 86.¹⁸ Kromě zákazu zasahování do soukromí jiného než ze zákonného důvodu také demonstrativně vyjmenovává možnosti zásahu do soukromí:¹⁹

- narušením soukromých prostor,
- sledováním soukromého života nebo pořizování záznamu o něm,
- využíváním záznamů o soukromém životě člověka pořízené třetí osobou,
- šířením takovýchto záznamů.

¹⁸ Část první, díl 2, oddílu 6 (Osobnost člověka), pododdíl 2 (Podoba a soukromí).

¹⁹ Použitím formulace „zejména“.

3.2 Právo na soukromí v ústavním pořádku a mezinárodních smlouvách

Ústavní zákon č. 2/1993 Sb., Listina základní práv a svobod (LZPS), zaručuje právo na soukromí v čl. 7 (odst. 1): „*Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.*“, čl. 10, odst. 2.: „*Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*“ a čl. 10 (odst. 3): „*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.*“

Listina základních práv Evropské Unie (2010/C 83/02), která má od přijetí Lisabonské smlouvy v roce 2009 stejný právní účinek jako zakládací smlouvy EU, obsahuje ochranu soukromého a rodinného života v čl. 7 a v čl. 8 speciálně ochranu údajů osobního charakteru.²⁰ Jde o odst. 1: „*Každý člověk má právo na ochranu údajů osobního charakteru, které se ho týkají.*“ a odst. 2: „*S těmito údaji musí být nakládáno čestně, pouze k přesně danému účelu a na základě souhlasu dotyčné osoby či na základě jiného legitimního opodstatnění uvedeného v zákoně. Každý člověk má právo na přístup k údajům sebraným o jeho osobě a na jejich zpřesnění.*“

Kromě Listiny základních práv EU je významná evropská Úmluva o ochraně lidských práv a základních svobod, vyhlášená jako č. 209/1992 Sb. ve znění pozměňujících protokolů (EÚLP), která byla ratifikována Československem v roce 1992 a která v čl. 8 zajišťuje právo na respektování soukromého a rodinného života.²¹

Mezinárodní pakt o občanských a politických právech, který byl publikovaný ve Sbírce zákonů jako vyhláška Federálního ministerstva zahraničních věcí č. 120/1976 Sb. upravuje právo na soukromí v čl. 17:

„*1. Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst.*“

²⁰ Na základě článku 6, odst. 1 Lisabonské smlouvy

²¹ Jde o dokument Rady Evropy. Na tento článek se odvolával nálezný ÚS popsany v kapitole 4.8 této práce.

2. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.

3.3 Obsah práv

3.3.1 Právo na soukromí

Přesnou definici obsahu práva na soukromí v zákonech nenajdeme – spíše jeho konkrétní ochranu. Například zákon č. 121/2000 Sb., o ochraně osobních údajů v § 4 definuje *osobní údaj* jako jakoukoliv informaci týkající se určeného nebo určitelného subjektu údajů, a také *citlivý údaj* jako osobní údaj vypovídající o národnostním či etnickém původu, politických a odborových postojích, zdravotním stavu a dalších.

Ochranu práva na soukromí poskytují také trestní předpisy – zvláštní část zákona č. 40/2009 Sb. trestního zákoníku, obsahuje ochranu osobnostních práv v hlavně II., dílu 2²², konkrétně ve skutkových podstatách trestných činů:

- § 180 – neoprávněné nakládání s osobními údaji,
- § 181 – poškození cizích práv,
- § 182 – porušení tajemství dopravovaných zpráv,
- § 183 – porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,
- § 184 – pomluva.

Z pohledu teorie člení Eliška Wagnerová právo na soukromý život do čtyř oblastí:²³

1. osobní soukromou sféru,
2. rodinný život, právo na uzavření manželství a založení rodiny,
3. soukromí v prostorové dimenzi (obydlí),
4. soukromí jako důvěrnost komunikace.

²² Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství

²³ ŠIMÍČEK, VOJTĚCH *Právo na soukromí* 1. vyd. Brno: Masarykova univerzita, 2011, 212 s. ISBN 978-80-210-5449-3, příspěvek JUDr. Elišky Wagnerové, PhD.: Právo na soukromí: Kde má být svoboda, tam musí být i soukromí

Pro účely této práce jsou nejvýznamnějšími první a poslední bod. S ochranou osobní soukromé sféry je spojováno též právo na ochranu před sledováním, hlídáním a pronásledováním veřejnou mocí – ať už jde o kamerové systémy či plošné sledování mobilních telefonů. Do osobní soukromé sféry řadí právo na informační sebeurčení (další kapitola) a autonomní rozhodování o osobní integritě.

Právo na informační sebeurčení lze popsat jako právo jednotlivce sám se rozhodnout, jaké informace o jeho vlastní osobě a za jakých okolností budou poskytnuty.²⁴ Tuto otázku rozpracoval podrobně Ústavní soud SRN v roce 1983 v otázce sčítání lidu s tím, že možnosti narušení tohoto práva jsou akceptovány pouze v případě převažujícího zájmu.²⁵

V otázce zásahů do práva na soukromí je významný *test proportionality*. Ten používá Ústavní soud, který tento test převzal od Evropského soudu pro lidská práva a používá se v případě poměrování konfliktu dvou práv a hodnot. Test proporcionality požaduje, aby dané omezení práva bylo **vhodné, potřebné a nesmí se vymykat poměru k dosahovanému cíli**.²⁶ Aby byl takový zásah považován za vhodný, tak je nutné, aby vykazoval věcnou souvislost s účelem nebo ho alespoň podporoval. Potřebnost předpokládá neexistenci mírnějšího prostředku.

²⁴ ŠIMÍČEK, VOJTĚCH *Právo na soukromí* 1. vyd. Brno: Masarykova univerzita, 2011, 212 s. ISBN 978-80-210-5449-3, příspěvek – Marian Kokeš, Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. Právo na soukromí: Kde má být svoboda, tam musí být i soukromí

²⁵ Rozhodnutí Spolkového soudu, BVerfGE 65, 1 z 15. 12. 1983

²⁶ Eliška Wagnerová, viz 23.

3.4 Související judikatura

3.4.1 Malone vs. Spojené království (1984)

V březnu 1977 byl James Malone, britský obchodník se starožitnostmi, obviněn z trestných činů v souvislosti s nakládáním se zbožím. Malone tvrdil, že po dobu několika let byla jeho poštovní korespondence i telefony odposlouchávány a podal žalobu k Evropskému soudu pro lidská práva.

Vláda Spojeného království sledování uznala za oprávněné a prohlásila, že probíhalo v souladu s právem. Sledování muselo být schváleno státním tajemníkem a bylo nutné splnit následující podmínky:²⁷

- spáchaný zločin musel být považovaný za závažný,
- standardní způsoby vyšetřování selhaly,
- musí být dostatečný předpoklad, že výsledek sledování povede k usvědčení.

Soud došel k názoru, že vnitřní zákony UK dostatečně přesně nespécifikovaly podmínky k odposlechu a konstatoval porušení čl. 8 Úmluvy. Speciálně zde bylo zmíněno „měření“ – ukládání dat o hovoru (volající, volané číslo, čas). Dle názoru soudu je i poskytnutí těchto dat porušením čl. 8 Úmluvy.²⁸

3.4.2 ÚS ČR – použitelnost zpravodajského odposlechu v trestním řízení

Český ústavní soud (ÚS) ve svém nálezu sp. zn. I. ÚS 3038/07 ze dne 29. 2. 2008, N 46/48 SbNU 549, Použitelnost odposlechu získaného dle zpravodajských zákonů v trestním řízení, řešil otázku, zda je možné použít odposlech získaný pro účely vojenského zpravodajství v trestním řízení.

Stěžovatelka se domáhala zrušení zahájení trestního řízení z důvodu porušení jejího práva na spravedlivý proces dle čl. 36 LZPS a práva na soukromí dle čl. 13 LZPS. Policie měla jako důkaz odposlechy získané v roce 2005 nikoliv dle § 88 trestního řádu, ale dle zákona č. 67/1992 Sb. o Vojenském obranném zpravodajství. Šlo

²⁷ Secretary of the State

²⁸ „Metering“

o trestné činy pokusu pletich proti veřejné soutěži a veřejné dražbě a týkající se hospodářského styku.²⁹

Útvar odhalování korupce a finanční kriminality SKPV Policie České republiky odmítal, že by odposlechy byly nepoužitelné, neboť dle § 89 odst 2. TrŘ může jako důkaz sloužit vše, co může přispět k objasnění věci (s výjimkou nezákonně získaných odposlechů). Stejně tak krajský státní zástupce konstatoval, že veřejný zájem na zjištění a potrestání by měl převážit nad zájmem na ochraně základních práv a svobod a že by zpravodajské odposlechy měly být použitelné, budou-li opatřeny záznamem splňujícím požadavky § 88 TrŘ.

ÚS konstatoval odlišné významy jednotlivých ustanovení zákonů (TrŘ a vojenského zpravodajství) – zatímco účelem úpravy je zjištění trestných činů a potrestání jejich pachatelů, v případě zpravodajských služeb jde o zabezpečení informací o záměrech a činnostech představující vojenské ohrožení ČR.

Dle ÚS by bylo popřením principů právního státu, kdyby záruky ústavnosti v trestním řízení bylo možné obejít aplikací zákonů o zpravodajských službách. Vzhledem k tomu, že v projednávané věci nečelila ČR bezprostřední hrozbě terorismu, nebyl zde důvod pro předání odposlechů PČR.

ÚS vyhověl stěžovateli v otázce vyřazení odposlechů z trestního řízení.

²⁹ Tento zákon byl zrušen 1. 8. 2005

4 Zákonná úprava a judikatura

Vzhledem k tomu, že zákonné normy procházejí stálým vývojem a to jak na úrovni EU, tak ČR, jsou následující kapitoly práce řazeny chronologicky a nikoliv dle typu práva (vnitrostátní, evropské).

Kvůli významu nálezů ústavních soudů (ČR i dalších zemí EU) a jejich dopadu na zákonnou úpravu jsou tyto nálezy umístěny také ve stejné části práce.

4.1 Provozní údaje v období před směrnicemi a vstupem do EU

Již před vstupem do EU a vznikem ZoEK s jeho novelami upravujícími mj. data retention (viz dále) existovala možnost, aby si policie vyžádala provozní údaje – typicky výpis hovorů. Policie si tato data zajišťovala jako listinný důkaz dle § 112 TrŘ.

4.1.1 Zákon o telekomunikacích

Zákon č. 151/2000 Sb., o telekomunikacích, obsahoval první zákonnou úpravu data retention – v § 86 odst. 1 stanovoval povinnost „sdělit orgánům oprávněným k tomu zvláštními právními předpisy informace o skutečnostech, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, zejména údaje o veškeré komunikaci, kteréhokoli uživatele v uplynulých nejméně dvou měsících v rozsahu volané a volající číslo, použitá služba, datum, čas, doba trvání komunikace a místo připojení“.³⁰

4.1.2 ÚS – Právo na ochranu zpráv podávaných telefonem

ÚS řešil problematiku poskytování provozních údajů v nálezu sp. zn. II. ÚS 502/2000 ze dne 22. ledna 2001, N 46/48 SbNU 549, Použitelnost odposlechu získaného dle zpravodajských zákonů v trestním řízení. V tomto případě byl stěžovatel uznán vinným z trestného činu loupeže s uložením trestu dvanácti let. Jako významný důkaz posloužil výpis hovorů dodaný společností EuroTel Praha (dnes O2).³¹ Součástí tohoto výpisu bylo také označení základnových stanic, tudíž bylo možné určit i polohu

³⁰ Byť se pro označení nepoužíval ani pojem data retention, ani provozní či lokalizační údaje.

³¹ Kromě toho ještě stěžovatel namítal další vady řízení, pro význam této práce je však důležitý zmiňovaný výpis hovorů.

telefonu. Stěžovatel namítal, že výpis hovorů nelze použít jako listinný důkaz, jak byl uváděn v řízení před soudy, ovšem vzhledem k jeho charakteru a důvěrnosti měla policie postupovat dle § 88 TrŘ. Vzhledem k tomu, že tak policie neučinila, navrhol prohlásit důkaz za nezákonný a tudíž absolutně neplatný.

ÚS konstatoval, že na tento výpis se vztahuje ochrana dle čl. 13 LZPS a zmínil přitom rozsudek Malone z roku 1984 (popsaný v kapitole 3.4.1) a důkaz prohlásil za protizákonný. Poznamenal, že měl být použit § 88 TrŘ, ovšem ještě vhodnější by byla speciální zákonná úprava, která však v této době chyběla.

Ke stejnému rozhodnutí dospěl ÚS také v nálezu sp. zn. IV. ÚS 536/2000 ze dne 13. 2. 2001, N 29/21 SbNU 251, Ochrana zpráv podávaných telefonem, v rozhodování ústavní stížnosti spolupachatele (šlo o stejný skutek).

Z důvodu vázanosti svými dřívějšími rozhodnutími ÚS také prohlásil za neplatné výpisy hovorů poskytnuté EuroTelem a RadioMobilem (dnes T-Mobile) a zrušil rozsudek vrchního soudu v trestní věci ve svém nálezu sp. zn. IV. ÚS 78/01 ze dne 27. 8. 2001, N 123/23 SbNU 197, K právu na ochranu zpráv podávaných telefonem - k otázce presumpce nevinny.

4.1.3 Novela trestního řádu

V návaznosti na rozhodnutí ÚS zařadili zákonodárci do novely trestního řádu zákonem 265/2001 Sb. nový § 88a, který speciálně vymezuje poskytování provozních dat (znění v zákoně: „*údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat*“). Takovéto poskytnutí dat musel nařídít předseda senátu či v přípravném řízení soudce. Tento paragraf byl pozdějším nálezem ÚS zrušen a zákonodárci opět upraven – viz další kapitoly této práce.

4.2 Evropské směrnice do roku 2006

Směrnice z roku 2002 upravující související problematiku ochrany osobních údajů č. 2002/58/ES ze dne 12. července 2002 – Směrnice o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací – zde upravuje v článku 6 především právo na soukromí účastníků – provozní údaje měly být uchovávány pouze pro účely účtování služeb a jen do konce období, kdy lze toto vyúčtování napadnout.

Možné bylo taktéž použít údaje pro marketing, pokud k takovému zpracování dali účastníci souhlas, typicky například při uzavírání účastnické smlouvy.

Stejně tak lokalizační údaje mohly být použity jen se souhlasu účastníků či po jejich anonymizaci.

V souladu s článkem 13 předchozí směrnice 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, však výše zmiňovaná směrnice v článku 15 povolovala i omezení těchto práv, pokud šlo o nezbytné, přiměřené a úměrné opatření pro zajištění:

- národní bezpečnosti,
- obrany,
- veřejné bezpečnosti a pro prevenci,
- vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému,
- významného hospodářského nebo finančního zájmu členského státu či EU,
- kontrolní, inspekční nebo regulační funkce z výkonu veřejné moci,
- ochrany subjektu údajů nebo práv a svobod druhých.

4.3 Zákon o elektronických komunikacích – první verze

4.3.1 Popis

Česká norma – zákon č. 127/2005 Sb., o elektronických komunikacích - upravuje široce oblast telekomunikací v ČR – z větší části hlavně zpracovává v předchozích kapitolách uvedené směrnice Evropského parlamentu a Rady a také další směrnice, které upravují dění na telekomunikačním trhu v EU.

Tento zákon řeší otázky, jakými jsou přístup k radiovým kmitočtům, přidělování a přenositelnost telefonních čísel, univerzální službu a veřejné telefonní automaty, digitální vysílání televize a rozhlasu, ale i například regulace cen a ochranu spotřebitele v této oblasti.

Pro data retention je zásadní hlava pátá, která upravuje ochranu dat a důvěrnost komunikací. V § 89 ZoEK je stanovena povinnost zajistit důvěrnost zpráv i s nimi spojených provozních a lokalizačních údajů – zakazuje také nezákonný odposlech a povoluje ukládání nezbytných technických údajů.

Samotná úprava data retention se v zákoně objevila již v první verzi z roku 2005 v § 97, konkrétní odstavce o data retention však byly později výrazně novelizovány. Konkrétní § 97 odst. 3 měl ve sněmovním tisku toto navrhované znění:

„Právnícká nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na vlastní náklady uchovávat provozní a lokalizační údaje a tyto údaje je na vlastní náklady a na vyžádání povinna poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu.“³²

Otázku oprávněných subjektů popisovala poznámka pod čarou určením zvláštních právních předpisů:

- trestní řád,
- zákon o Policii ČR,
- zákon o BIS,
- zákon o Vojenském obranném zpravodajství.

4.3.2 Zákonodárny proces

Zákon předložila vláda sněmovně v září 2004.

Z úpravy týkající se data retention došlo při projednávání k následujícím změnám:

- Výbor pro obranu a bezpečnost navrhl omezit oprávněné subjekty (viz dále) a shodl se na tom, že odposlechy (a s nimi související data retention) by měly být řešeny komplexně v tzv. protiteroristickém zákonu, který však v ČR nikdy nevzniknul.

³² Sněmovní tisk 768/0 ze dne 8. září 2004

- Hospodářský výbor změnil financování nákladů – z původního návrhu, dle kterého měli náklady hradit poskytovatelé, došlo ke změně a náklady na data retention nyní platí stát.

Ministr informatiky Vladimír Mlynář při druhém čtení v prosinci 2004 zdůraznil, že jde o normu nutnou z důvodu sjednocování regulačního rámci spolu s EU a že ČR je jedna z pěti zemí EU, kde norma stále chybí. Z toho důvodu zahájila EU *infringement procedure*, a následně ministr Mlynář žádal o zkrácení lhůty mezi druhým a třetím čtením. Ve veřejné rozpravě zaznělo mnoho pozměňovacích návrhů např. kvůli digitalizaci televizního vysílání či telefonním seznamům, ovšem žádný z nich se netýkal data retention (stejně tak pozměňovací návrhy po druhém čtení, sněmovní tisk č. 768/5, neobsahuje žádné změny § 97 souvisejících s touto schůzí). Ve třetím čtení Vladimír Mlynář podpořil návrhy Výboru pro obranu a bezpečnost – další diskuze kolem zákona se pak již týkala jiných témat.

V hlasování pak návrh zákona prošel 17. prosince 2004 poměrem 108:54 – téměř jednotně pro byli poslanci ČSSD, KSČM a US-DEU, naopak ODS z celkových 54 odmítavých hlasů měla 49. Zákon byl vyhlášený 31. března 2005 s účinností od 1. května 2005.

4.3.3 Provozní údaje a lokalizační údaje a prováděcí vyhláška

ZoEK přinesl také definici těchto pojmů.

Provozní údaje jsou definovány jako „*jakékoliv údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování*“.

Lokalizační údaje pak jsou definovány jako „*jakékoliv údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací*“.

Vzhledem k tomu, že definice provozních údajů je poměrně široká, konkrétní detaily, jaké údaje je nutné policii poskytovat, řešila vyhláška 485/2005 Sb. ze 7. prosince 2005 od Ministerstva informatiky.³³

Další odstavce § 90 upravují možnosti, které poskytovatel má se zpracováním provozních údajů – otázky ukládání dat pro účtování služeb, pro marketing a otázku poskytování služeb. Patří sem například povinnost ukládat provozní údaje po dobu, kdy je možné právně napadnout vyúčtování služeb a taky následnou povinnost tato data zlikvidovat. Pro marketing mohou být využívána pouze s předchozím souhlasem uživatele, který může tento souhlas kdykoliv odvolat.

4.3.4 Policie a další oprávněné subjekty

V první schválené verzi ZoEK v roce 2005 v § 97/1 byla stanovena povinnost operátora zřídit rozhraní pro odposlech a záznam zpráv pouze pro Policii ČR³⁴.

Za zmínku ale stojí, že dle prvního návrhu zákona část § 97/1, která vyjmenovává oprávněné subjekty, zněla následovně:

... síť rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv:

- a) Policii České republiky pro účely stanovené zvláštním právním předpisem,*
- b) Bezpečnostní informační službě pro účely stanovené zvláštním právním předpisem,*
- c) Vojenskému zpravodajství pro účely stanovené zvláštním právním předpisem,*
- d) Úřadu pro zahraniční styky a informace pro účely stanovené zvláštním právním předpisem.³⁵*

³³ Vzhledem k tomu, že tato vyhláška byla později zrušena, popisuje tato práce pouze aktuálně platnou vyhlášku č. 357/2012 Sb.

³⁴ Otázka oprávněných subjektů u odposlechů se později ukázala důležitá i pro data retention, kde nebyly subjekty takto jednoznačně specifikovány. – viz kapitola 4.8.2 o nálezu ÚS

³⁵ Sněmovní tisk č. 768/0

Výbor pro obranu a bezpečnost doporučil ve svém usnesení BIS, Vojenské zpravodajství a Úřad pro zahraniční styky a informace ze seznamu oprávněných subjektů vyškrtnout.

Tato povinnost byla následně rozšířena o BIS a Vojenské zpravodajství až zákonem č. 290/2005 Sb. Samotné ukládání tedy bylo v prvním znění zákona určeno v § 97/3: *“Právnícká nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službou elektronických komunikací je povinna uchovávat provozní a lokalizační údaje a tyto údaje je na požádání povinna poskytnout orgánům oprávněným k jejich využívání, stanoví prováděcí právní předpis.“*

Také zde byla stanovena povinnost údaje poskytovat ve srozumitelné podobě i pro případ, že poskytovatel používá kódování či kompresi.

4.4 Směrnice 2006/24/ES

Až směrnice 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí z 15. března 2006 však přinesla jednoznačnou a konkrétní povinnost členským státům zavést uchovávání dat do právních řádů jednotlivých zemí.

4.4.1 Důvody pro přijetí směrnice

Mezi důvody, které vedly k přijetí směrnice, byly:

- fakt, že některé členské státy již takové zákony přijalo,³⁶
- sjednocení pravidel na vnitřním trhu elektronických komunikací,
- závěr zasedání Rady pro spravedlnost a vnitřní věci, ve kterém bylo konstatováno, že elektronické komunikace jsou důležité pro předcházení a vyšetřování trestných činů a organizované trestné činnosti v prosinci 2002,
- prohlášení o boji proti terorismu z března 2004, ve kterém bylo Radě uloženo prověření opatření pro uchovávání provozních údajů,

³⁶ Šlo například o Itálii, kde začal zákon platit v červenci 2005 nebo zmiňovaný český ZoEK

- požadavky článku 8 EÚLP, který specifikuje možnost státních orgánů zasahovat do práv na respektování soukromého a rodinného života jen z vyjmenovaných důvodů,
- prohlášení Rady EU z července 2005, kdy po teroristických útocích v Londýně byla potvrzena potřeba přijetí společných opatření v otázce uchovávání telekomunikačních údajů.

4.4.2 Obsah směrnice

Nově zavedená povinnost uchovávání dat nemá vliv na články 5, 6 a 9 existující směrnice 2002/58/ES – ta byla také touto směrnicí novelizována odstavcem, který z její účinnosti vyjímá sledování pro data retention.

Jako velmi problematické bylo považováno neurčitě definovaný účel ukládání dat – dotýká se ho pouze článek 1 v následujícím znění:

„Účelem této směrnice je harmonizovat předpisy členských států týkající se povinnosti 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, jak jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech.“

Speciálně v článku 5 jsou stanovené kategorie uchovávaných údajů – tedy údaje k identifikaci zdroje i adresáta spojení, zjištění data, času a doby trvání komunikace a také určení typu spojení, polohy uživatele. Důležitý je zákaz uchovávání obsahu sdělení v druhém odstavci článku 5.

Doba uchovávání byla stanovena na minimálně šest měsíců a maximálně dva roky ode dne komunikace.

Základními zásadami, které měly být dodržovány z pohledu bezpečnosti a ochrany údajů, šlo o:

- uchovávané údaje měly mít stejnou kvalitu a také podléhat stejnému zabezpečení a ochraně jako údaje na síti,

- na uchovávané údaje se vztahovala přiměřená technická a organizační opatření před zničením, ztrátou, pozměněním, zveřejněním či obdobnou manipulací,
- k údajům mohly přistupovat pouze zvlášť zmocněné osoby,
- na konci doby uchovávaní se data zničila (kromě těch, která byla zajištěna).

Každý členský stát musel na základě směrnice určit alespoň jeden orgán veřejné moci, který měl na starosti dodržování předpisů, a tyto orgány měly působit zcela nezávisle.

Komise musí alespoň jednou ročně dostat statistiku případů, kdy byly příslušným orgánům poskytnuty informace, spolu s údajem o čase, který uplynul mezi uchováním údaje a jeho poskytnutím.

Samotný způsob provedení směrnice byl ponechán na jednotlivých členských státech a jako termín nabytí účinnosti, byl stanoven 15. září 2007. Dvouletá výjimka byla stanovena na uchovávaní údajů týkajících se internetových služeb (připojení k internetu, internetová telefonie a elektronická pošta). ČR oznámila, že tuto úpravu přijme do 36 měsíců od přijetí této směrnice.

4.4.3 Odpor proti směrnici 2006/24/ES

Pracovní skupina 29 byla zřízena článkem 29 směrnice 95/46/ES jako nezávislý orgán s poradní funkcí. Tvoří ji zástupce orgánu dozoru jednotlivých členských států či institucí EU a mezi její úkoly patří posuzování otázek týkajících se uplatňování směrnice a vyjadřuje se k návrhům na změny. Členem za Českou republiku je RNDr. Igor Němec, předseda Úřadu pro ochranu osobních údajů (ÚOOÚ).

Již v průběhu zákonodárského procesu v říjnu 2005 vyjádřila skupina své výhrady. Šlo o konstatování bezprecedentního zásahu do lidských práv a svobod z toho důvodu, že postihuje každého občana a vyjádřila obavu, že může jít o ohrožení základních hodnot – práva na soukromí a práva na informační sebeurčení. Skupina v návrhu směrnice postrádala dostatečné bezpečnostní pojistky a varuje před možností významných odchylek v jednotlivých státech.

Speciálně zmiňovala velmi neurčitě definovaný účel ukládání dat a považovala za nutnost zaznamenávat přístupy k těmto údajům a zpřístupnit je kontrolnímu orgánu.

4.5 Novela zákona v roce 2008

V ČR představovalo výraznou změnu úpravy DR zákon č. 247/2008 Sb., který novelizoval § 97:

- k povinně předávaným údajům byly zařazeny i neúspěšné pokusy o volání (tzv. *prozvánění*), jsou-li tyto záznamy vytvářeny
- speciálně bylo zakázáno s těmito údaji uchovávat obsah zpráv
- lhůta pro ukládání dat byla stanovena mezi 6-12 měsíci a byla zavedena povinnost tato data následně zlikvidovat.

Za zmínku stojí, že již při přijímání této novely zazněly i nesouhlasné názory, např. poslance Milana Urbana, který kritizoval sledování a tvrdil, že zákon omezuje svobodu v ČR. Oproti tomu František Bublan namítal, že přidané sledování *prozvánění* nepředstavuje významnější zásah do soukromí a že takovéto údaje pomohly při odhalení atentátníků v Londýně.³⁷

Po následné diskuzi pak návrh prošel do druhého čtení a později byl ve třetím čtení poměrem 89:21 schválen.

4.6 Rozsudek SD EÚ z února 2009

V červenci 2009 podalo Irsko spolu se Slovenskem žalobu na neplatnost směrnice 2006/24/ES. Proti této žalobě byl Evropský parlament, Rada EU a dále Španělsko, Nizozemí, Komise ES a Evropský inspektor ochrany údajů.

Důvodem pro neplatnost žaloby bylo tvrzení, že nebyla přijata dle náležitého právního základu – konkrétně neměl být dle tvrzení Irska použit článek 95 Smlouvy o fungování ES (standardní legislativní proces), ale článek 30 a následující Smlouvy o fungování EU (společný postup v oblasti policejní spolupráce), neboť hlavním cílem data retention má být vyšetřování kriminality. Slovensko také namítalo výrazný zásah do čl. 8 Evropské úmluvy o lidských právech, který neměl být upraven podle čl. 95.

³⁷ Poslanec a v období srpen 2004 – září 2006 ministr vnitra

Oproti tomu Parlament ani Rada neviděly v použití čl. 95 vadu – směrnice upravuje i jiné záležitosti a potřeba potírat trestnou činnost nevádí přijetí tímto způsobem. Další argumentace pro směrnici se týkala faktu, že jedním ze základních cílů bylo odstranění překážek na vnitřním trhu harmonizací vnitrostátních předpisů a že změny, které byly provedeny, lze provést pouze prostřednictvím aktu Společenství a ne aktu dle SFEU.³⁸

Žaloba podaná Irskem se týkala pouze volby právního základu a nikoliv otázky případného porušení lidských práv – z toho důvodu Soudní dvůr ve velkém senátu žalobu zamítl.

4.7 Rozhodnutí Spolkového ústavního soudu v roce 2010

Německý telekomunikační zákon upravující mj. data retention (Telekommunikationsgesetz – *TKG*) byl přijatý v prosinci 2007 na základě směrnice 2006/24/ES a zavedl povinnost uchovávat data po dobu minimálně půl roku a maximálně dvou let spolu s povinností jejich poskytnutí pro vyšetření závažných trestných činů.

Stěžovatelé namítali rozpor právní úpravy s německou ústavou (Grundgesetz für die Bundesrepublik Deutschland), konkrétně s článkem 10, který stanoví nedotknutelnost soukromí korespondence, pošty a telekomunikací (byť článek 2 umožňuje omezení na základě zákona, podobně jako například česká úprava) a článkem č. 12 umožňující svobodnou volbu povolání.

S druhým zmiňovaným článkem se soud neztotožnil – speciální povinnosti v telekomunikacích nepovažoval za dostatečný problém podnikání v této oblasti, ovšem nesoulad s článkem 10 potvrdil.

³⁸ SFEU = Smlouva o fungování Evropské unie

Ústavní soud dospěl k názoru, že úprava je protiústavní a v březnu 2010 zmiňované paragrafy TKG zrušil – hlavním důvodem byla obava z plošného sledování obyvatel.

Zajímavým faktem v rozhodnutí je, že skutečnost, že data nejsou shromažďována státem, mluví dle rozhodnutí soudu spíše ve prospěch zákona (směrnice), neboť neposkytují centrální databázi na státní úrovni, ale jsou uložena u jednotlivých poskytovatelů a tím snižují riziko zneužití. Jiné soudy totiž (viz následná rozhodnutí) v tomto viděly problém ve zneužití dat poskytovatelem či jeho zaměstnanci oproti údajně bezpečnějšímu uložení dat u státních orgánů.

Více než dva roky po tomto rozsudku podala Komise žalobu k Soudnímu dvoru EU s navrhovanou pokutou více než 300 tisíc eur denně, které mělo Německo platit pro nesplnění implementace směrnice zavádějící data retention. V době psaní této práce nebylo o žalobě rozhodnuto, vzhledem ke zrušení směrnice (viz kapitola 4.11) je však udělení pokuty velmi nepravděpodobné.

4.8 Nález Ústavního soudu ČR z roku 2011

V březnu 2010 podala skupina 51 poslanců návrh Ústavnímu soudu, ve kterém se domáhala zrušení ustanovení § 97 odst. 3 a 4 ZoEK a prováděcí vyhlášky.

Ústavní soud samotný návrh na zrušení zákona přijal k projednání, byť konstatoval výtku, že zákonodárci mají sami možnost upravit zákon, který považují za protiústavní a je výrazně nestandardní, pokud návrh předkládají poslanci vládní koalice, obzvláště v případě, že jich část pro zákon sama hlasovala.

Navrhovatelé tvrdili, že data retention v aktuální podobě je v rozporu s článkem č. 8 Úmluvy o ochraně lidských práv a svobod, která dává každému právo na respektování jeho soukromého života, obydlí a korespondence. Možnost zásahů od státu je možná pouze v případě zákona, a to v zájmu národní bezpečnosti, blahobytu země apod. (odstavec 2 Úmluvy).

Dále v data retention považovali navrhovatelé nebezpečí v omezení základních práv nejen samotným seznámením se s údaji, ale jejich plošným uchováváním a tedy možností vyžádat si jejich obsah zpětně. Dalším problémem bylo, že data neuchovává sám stát, ale velké množství soukromých subjektů a tedy výrazně narůstá riziko zneužití dat. Občan se plošnému sledování neměl jak vyhnout a šlo z něho zjistit mnoho informací o jeho osobě (i bez znalosti předávaných zpráv).

Ačkoliv je samotná otázka zrušení zákona problematikou vnitrostátní, data retention vychází z komunitárního práva. Proto navrhovatelé předestřeli ÚS možnost předběžné otázky Evropskému soudnímu dvoru z důvodu otázky neplatnosti celé směrnice, neboť viděli rozpor nejenom s českým právním řádem, ale i právem EU.

Nejprve se ÚS zabýval návrhem předložení předběžné otázky Evropskému soudnímu dvoru týkající se neplatnosti celé směrnice o data retention.

Následně ÚS konstatoval, že ačkoliv nelze pominout vliv komunitárního práva, jde primárně o otázku české ústavnosti a řeší se konkrétní podoba české transpozice, tedy zákona a vyhlášky.

ÚS si vyžádal vyjádření od Poslanecké sněmovny, Senátu a Veřejného ochránce práv. Poslanecká sněmovna (zastoupena předsedou) tvrdila, že přijatý zákon je v souladu s ústavním pořádkem, Senát (také zastoupený předsedou) rovněž potvrdil, že návrh zákona schválil, a speciálně připomněl, že Senát souhlasil s návrhem předkladatele, že se uchovávají pouze technická data a tudíž nejde o zásah do soukromí, který by šlo připodobnit k odposlechům. Veřejný ochránce práv se s návrhy předkládanými k ÚS neztotožnil, a proto se k řízení nepřipojil.

ÚS posuzoval:

- právo na respekt k soukromému životu a na informační sebeurčení,
- přípustnost zásahu do tohoto práva.

4.8.1 Soukromí

ÚS připomněl článek 8 Úmluvy o ochraně lidských práv a základních svobod článek 10, odst. 2 Listiny, dle kterých má každý právo na ochranu před neoprávněným

zasahováním do soukromého života a odstavec 3 chráníci jednotlivce před neoprávněným shromažďováním, zveřejňováním či zneužíváním údajů o jeho osobě.

4.8.2 Přípustnost zásahů

Primární cílem přístupu k operátory posbíraných dat z preventivního sběru dat je ochrana před bezpečnostními hrozbami a odhalování a stíhání trestných činů, což ÚS považuje za veřejný zájem; ovšem umožňuje-li trestní právo zásahů do soukromí, může k tomuto zásahu dojít jen zcela výjimečně a nelze-li tohoto záměru dosáhnout jinak. Musí být přítom také splněné záruky dostatečné kontroly a přezkoumatelnosti nezávislým soudem. Tento požadavek se projevuje vydáním soudního příkazu a jeho dostatečným odůvodněním.

ÚS se také odvolával na svoji dřívější judikaturu (např. nález ÚS 502/2000 o právu na ochranu zpráv podávaných telefonem a nález ÚS 3038/07 o použitelnosti odposlechu získaného dle zpravodajských zákonů v trestním řízení)³⁹, ve které zdůraznil možnost zásahu pouze na základě jasné imperativní zákonné normy, která splňuje požadavky testu proporcionality, konkrétně:

- naplnění účelu a vhodnosti
- posouzení potřebnosti (nejšetnější použitý prostředek)
- přiměřenosti (zda není újma zásahu nepřiměřená vzhledem k zamýšlenému cíli)

ÚS také zmínil práci *MIT* (Massachusetts Institute of Technology), která tvrdí, že i bez znalosti uchovávané komunikace lze na základě dat o provozu zjistit, kde se jednotlivec stýká, kdo jsou jeho nejbližší známí, kolegové z práce apod.

4.8.3 Názor ÚS na právní úpravu

Ústavní soud došel k názoru, že aktuální zákonná úprava neodpovídala ústavněprávním požadavkům a to z následujících důvodů:

- § 97 odst. 3 ZoEK: „...na požádání je bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu.“ dle soudu ani spolu s prováděcí vyhláškou dostatečně přesně nekonkretizovala, o jaké

³⁹ Popsané v kapitole 4.1.2

oprávněné orgány jde. Pouze na základě § 97 odst. 1, jež stanovuje povinnost provozovatelům zřídit rozhraní pro připojení zařízení pro odposlech a záznam zpráv konkrétním subjektům, šlo dovodit, že jde o stejné subjekty jako v případě odst. 3 – tedy OČTŘ (§ 88a trestního řádu), BIS a Vojenské zpravodajství.

- Účel, pro který mají být údaje poskytovány, nepovažuje soud za dostatečně určený a tudíž ani předvídatelný – Směrnice o data retention vymezuje jako cíl vyšetřování, odhalování a stíhání zvláště závažných trestných činů (ovšem bez jejich vymezení), česká úprava nemá žádné vymezení. ÚS došel k názoru, že je nutné přesně vymezit, pro které trestné činy (zvláště závažné) je možné data retention použít. Dle statistik docházelo k nadužívání tohoto instrumentu i pro odhalování a stíhání méně závažných trestných činů. (Pro srovnání dle Zprávy o bezpečnostní situaci v ČR citované v nálezu ÚS bylo zjištěno 343 tisíc trestných činů a počet žádostí v tomto období dosáhl 131 tisíc.)
- Zcela nedostatečně je dle ÚS řešena ochrana údajů – konkrétně přístupu třetích osob či jejich zničení.

4.8.4 Rozhodnutí

Ústavní soud konstatoval ustanovení § 97 odst. 3 a 4 ZoEK a vyhlášku 485/2005 Sb. za ústavně nekonformní a zrušil je na základě § 70 odst. 1 Zákona o ÚS k 31. 3. 2011 (den vyhlášení). Ve sbírce byl nález publikován pod číslem 94/2011 Sb (nález sp. zn. Pl ÚS 24/10 ze dne 22. března 2011, č. 94/2911 Sb., Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu).

4.8.5 Obiter dictum

ÚS si byl vědom toho, že s rozvojem moderních technologií dochází k výskytu nových způsobů páchaní trestné činnosti, ovšem vyjádřil pochybnosti, zda data retention je přiměřený způsob boje s trestnou činností a zda není vhodnější nástroj např. tzv. *data freezing*, který se od data retention liší sbíráním dat u konkrétní předem určené osoby.

Také vyjádřil pochybnosti nad tím, zda jde o efektivní nástroj při existenci tzv. anonymních SIM karet, které dle vyjádření Policie ČR jsou využívány až při 70 % trestné činnosti.⁴⁰

Otázkou také dle ÚS zůstává, zda je v pořádku, že soukromé osoby (operátoři) mohou uchovávat tato údaje a používat je pro účely marketingu či vymáhání pohledávek, tedy že v zákoně nejsou dostatečně vymezeny mantinely ani kontrolní mechanismy.

4.8.6 Druhý náleží Ústavního soudu

Obvodní soud pro Prahu 6 podal v květnu 2011⁴¹ návrh na zrušení § 88a trestního řádu poté, co před ním probíhalo řízení o návrhu Vojenské policie na vydání příkazu ke sdělení údajů dle § 88a trestního řádu.

Obvodní soud se domníval, že nemůže rozhodnout z důvodu rozporu ustanovení s ústavním pořádkem a odkazoval se na rozhodnutí ÚS Pl. ÚS 24/10 (předchozí kapitola).

ÚS na základě obdobné argumentace (hlavně z důvodu absence proporcionality) jako u Pl. ÚS 24/10 rozhodl o zrušení § 88a v prosinci 2011, ovšem dal zákonodárcům delší čas na úpravu zákona posunutím derogace až na 30. září 2012 (sp. zn. Pl. ÚS 42/11 ze dne 20. prosince 2011, vyhlášený pod 43/2012 Sb.).

Závěrem však ÚS podotknul, že jeho krok nelze vykládat tak, že každá aplikace § 88a by měla za následek porušení práva uživatelů na soukromí, ani že žádné použití získaných údajů nelze použít před soudem v dokazování v trestním řízení. Byl však přesvědčen, že aktuální nedostatky vytvářely prostor pro nepřiměřený či svévolný postup OČTŘ při nakládání s údaji a je nutná nová úprava od zákonodárce.

⁴⁰ V ČR, na rozdíl od některých jiných zemí EU, např. Slovenska, není povinnost se při koupi předplacené SIM karty registrovat.

⁴¹ Tedy v době, kdy bylo poskytování provozních a lokalizačních údajů rozhodnutím ÚS už 2 měsíce zrušeno.

4.9 Novela ZoEK v roce 2012

Na nálezu ÚS zareagovali zákonodárci novelou ZoEK, konkrétně zákonem č. 273/2012 Sb, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (ZoEK), ve znění pozdějších předpisů, a některé další zákony.

Vládní návrh, který vláda předložila sněmovně 27. 2. 2012, počítal s úpravami ZoEK:

- úpravou § 88a TrŘ, dle kterého má osoba provozující komunikační síť povinnost, aby provozní a lokalizační údaje měly stejnou kvalitu a ochranu před neoprávněným přístupem, zničením apod. jako údaje dle § 88 (tedy standardní telekomunikační provoz bez poskytování údajů). Spolu s tím také stanovuje povinnost připravit vnitřní předpis pro zaměstnance.
- s navrácením § 97 odst. 3 ZoEK a v jeho textu přesným vymezením oprávněných orgánů (OČTŘ, PČR při pátrání po hledané osobě či zjišťování totožnosti a odhalování nebo předcházení terorismu, BIS, ČNB a Vojenském zpravodajství)
- novým § 97 odst. 4 (rozsah a způsob předávání údajů stanoví prováděcí předpis)
- novým § 118 odst. 14 (nesplnění povinnosti dle § 88a je správní delikt)

Další úpravy měly zahrnovat rozsáhlou úpravou § 88a TrŘ:

- přesným určením trestných činů, pro které lze žádat o poskytnutí dat:
 - úmyslný trestný čin s horní hranicí trestu odnětí svobody na nejméně tři roky⁴²
 - TČ porušení tajemství dopravovaných zpráv (§ 182)
 - TČ podvodu (§ 209)
 - TČ týkající se neoprávněných přístupů k počítačovému systému (§ 230, § 231)
 - TČ nebezpečného vyhrožování a pronásledování (§ 353, § 354)

⁴² Tato horní sazba také odpovídá možnosti vzít osobu do vazby dle § 68 odst 2. trestního řádu

- TČ šíření poplašné zprávy (§ 357)
- TČ podněcování k trestnému činu nebo schvalování (§ 364, § 365)
- úmyslný TČ, jehož stíhání zavazuje vyhlášená mezinárodní smlouva
- určením procesu pro žádání:
 - v řízení před soudem vydání nařídí předseda senátu (v přípravném řízení soudce) státnímu zástupci nebo policejnímu orgánu na návrh státního zástupce
 - žádost musí být podána písemně, musí být odůvodněna a uvedena totožnost uživatele, je-li známa
- Předseda senátu, policejní orgán nebo státní zástupce musí po pravomocném skončení věci informovat uživatele o nařízeném zjišťování údajů o telekomunikačním provozu, pokud je tato osoba známa. Součástí této informace je také poučení o právu podat Nejvyššímu soudu návrh na přezkoumání zákonnosti tohoto příkazu.

Výjimku tvoří řízení o zločinu, jehož horní sazba je minimálně 8 let, spáchaném organizovanou skupinou, nebo jde-li v řízení o více osob (potenciálních spolupachatelů) a jejich řízení nebylo pravomocně skončeno. Také nebude podána informace, pokud by došlo ke zmaření trestního řízení nebo ohrožení bezpečnosti státu, života, zdraví, prac nebo svobod osob.

Pro srovnání s dřívějším zněním § 88a trestního řádu šlo o mnohem přesnější vymezení důvodů, pro které lze žádat vydání dat.⁴³

⁴³ Znění § 88a před zrušením nálezem ÚS: *(1) Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnícké nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.*

Další navrhované změny zákona se týkaly zákona o Bezpečnosti informační službě (poskytnutí provozních nebo lokalizačních údajů a jejich postavení na stejnou úroveň s odposlechy v § 8a), zákona o dohledu v oblasti v kapitálového trhu (na základě povolení předsedy senátu vrchního soudu dle sídla ČNB pro odhalení správního deliktu souvisejícího s kapitálovým trhem v dle § 8 odst. 1) a zákona o Vojenském zpravodajství (§ 9, obdobně jako u BIS).

Navrhovaná účinnost nové úpravy byla od 1. října 2012 (30. září 2012 měl přestat platit § 88a trestního řádu na základě nálezů ÚS).

Důvodová zpráva popisovala, že vládní návrh je reakcí na nálezy ÚS a kromě základního popisu problematiky také obsahovala příklady úspěšného využití data retention, kdy byly díky výpisu z buněk mobilní sítě vytipováni pachatelé sériové majetkové trestné činnosti.

Dále jsou uvedené změny, kterými návrh reaguje na výtky ÚS – např. vymezením trestných činů, u nichž může být žádáno o poskytnutí dat.

V prvním čtení se k návrhu vyjádřil poslanec Marek Benda, který byl jedním ze skupiny poslanců, kteří iniciovali nálezy ÚS. Návrhu vytkl hlavně část týkající se trestných činů – dle jeho názorů měl být § 88a používán v případě závažných trestných činů, ovšem dle názoru Ministerstva vnitra je závažným trestným činem „úplně všechno“, včetně šíření zprávy na internetu. Proto chtěl další debatu nad hranicí 3 let (horní sazba úmyslného trestného činu, kde lze použít data retention).

(2) Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.

Poslanec David Rath byl naopak proti návrhu jako celku (proti plošnému sledování osob) a pokud už je nutné k návrhu přikročit, pak chtěl debatovat nad vymezením trestných činů a doby, kdy lze data vyžádat.

Po obecné rozpravě byl návrh zákona postoupen výboru pro bezpečnost.

Výbor pro bezpečnost i ústavně právní výbor svými usneseními z května 2012 doporučil sněmovně návrh zákona schválit.

V druhém čtení 14. června 2012 došlo k pouze technickým pozměňovacím návrhům. Návrh obhajoval ministr vnitra Jan Kubice, pro návrh se postavil také například poslanec Viktor Paggio, který chválil nově nastavené bezpečnosti pojistky.

S návrhem zákona souhlasilo 20. června 2012 154 přítomných poslanců (ze 168), proti nebyl nikdo. Senátem zákon prošel 18. července 2012, prezident návrh podepsal 1. srpna 2012 a byl dodržen termín původně zamýšlené účinnosti – k 1. říjnu 2012. Od tohoto data je tedy povinnost operátorů v ČR poskytovat provozní a lokalizační oprávněným subjektům opět platné.

Nová prováděcí vyhláška stanovující rozsah provozních a lokalizačních údajů připravená Ministerstvem průmyslu a obchodu nabyla účinnosti od 1. listopadu 2012 s výjimkou některých technických ustanovení, které začaly platit od 1. ledna 2013. Podrobnější informace o jejím obsahu naleznete v kapitole 5.1 této práce.

4.10 Stanovisko generálního advokáta Soudního dvoru EU

Dalším významným mezníkem pro data retention byly rozhodnutí na evropské úrovni. Generální advokát má u Soudního dvoru Evropské unie (*SD EU*) za úkol předkládat stanoviska k případům předloženým soudy.

Na *SD EU* se v řízení o předběžné otázce obrátily dva soudy, konkrétně irský High Court of Ireland a rakouský Verfassungsgerichtshof.

U irského soudu šlo o rozhodnutí ve sporu mezi irskými orgány a společností Digital Rights Ireland Ltd., která namítala, že irské orgány zpracovávaly údaje vzniklé

při komunikaci mobilního telefonu společnosti. Tato žaloba k High Court byla podána v srpnu 2006, k SD EU došla žádost o rozhodnutí o předběžné otázce v červnu 2012.

High Court položil Soudnímu dvoru předběžné otázky týkající se slučitelnosti směrnice č. 2006/24/ES:

- s právem občanů svobodně se pohybovat a pobývat na území členských států (čl. 21 SFEU),
- s právem na respektování soukromého života (čl. 7 Listiny a čl. 8 EÚLP),
- s právem na ochranu osobních údajů (čl. 8 Listiny),
- s právem na svobodu projevu (čl. 11 Listiny a čl. 10 EÚLP),
- s právem na řádnou správu (čl. 41 Listiny).

V případě rakouského soudu šlo o tři návrhy, které tvrdily, že zákon o telekomunikacích je v rozporu s rakouskou ústavou – k tomuto návrhu se přidalo dalších 11 130 navrhovatelů. K SD EU došla žádost o rozhodnutí o předběžné otázce v prosinci 2012. Šlo o pět předběžných otázek týkajících se výkladu smluv a výše popsané irské otázky byly nakonec pro rozhodnutí klíčovější.

Generální advokát Pedro Cruz Villalón dospěl ve svém stanovisku v prosinci 2013 k závěru, že směrnice č. 2006/24/ES je v rozporu s Listinou základních práv Evropské unie.

U předběžných otázek High Courtu se zaměřil především na zkoumání souladu s čl. 7 a čl. 8 Listiny základních práv EU.

Směrnici považuje za zásah do soukromí a práva na ochranu osobních údajů – nejzávažnější otázkou je ale fakt, že údaje jsou zpracovávány soukromými společnostmi. Vzhledem k tomu, že generální advokát konstatoval zvláště závažný zásah do soukromí zkoumal její platnost a proporcionalitu z hlediska základních práv.

Generální advokát dále rozdělil svoje stanovisko na tři části:

- otázka proporcionality směrnice,

- omezení výkonu základních práv bylo „dle zákona“ tedy za splnění podmínky čl. 52 Listiny,
- proporcionalita směrnice ve spojení s čl. 52

4.10.1 Proporcionalita směrnice

V této části generální advokát vychází z dřívějšího rozsudku SD EU o právním základu směrnice – konstatoval, že využití směrnice pro trestní otázky, byť její hlavní funkcí je harmonizace vnitřního, není zjevně nepřiměřená sledovanému cíli.

Tím však konstatuje její právní základ, zároveň však říká, že stejné důvody mohou způsobit problém v otázce proporcionality dle čl. 5 odst. 4 SEU.⁴⁴

I s ohledem na dřívější rozsudek však definitivně nerozhodl o proporcionalitě v první části svého stanoviska s tím, že vyřešení tohoto problému není pro stanovisko závazné.

Zmínil zde však další části klíčové pro rozhodnutí:

Díky tomu, že směrnice č. 2006/24/ES stanoví rozsáhlé povinnosti operátorům sběru dat a zároveň ponechává záruky na členských státech – bude nutné posoudit i toto hledisko.

Také s ohledem na intenzitu sběru dat měla směrnice alespoň načrtnout skupiny trestných činů či přísnější podmínky přístupu k nim podobně jako například u práva na lékařské tajemství.

Unijní zákonodárce měl také usměrnit členské státy při přijímání zákonů tak, aby každý přístup k nashromážděným údajům byl omezen na soudní nebo alespoň jiné nezávislé orgány nebo alespoň aby každá žádost podléhala kontrole za strany soudů.

Sledování občané měli být také zpětně informováni o takovém přístupu.

⁴⁴ Smlouva o EU, čl. 5 odst. 4: „Podle zásady proporcionality nepřekročí obsah ani forma činnosti Unie rámec toho, co je nezbytné pro dosažení cílů Smluv.“

4.10.2 Omezení výkonu práv dle čl. 52 Listiny práv Evropské unie

Shromažďování údajů dle směrnice musí splňovat požadavek čl. 52 Listiny základních práv Evropské unie, který stanoví: *„Každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.“*

Otázka se díky směrnici přesouvá na vnitrostátní úroveň, protože směrnice předpokládá určení její povinnosti zákonem členského státu (jako v ČR např. ZoEK).

Cíl samotné směrnice – zajištění dostupnosti shromážděných a uchovávaných údajů pro účely odhalování závažných trestných činů – je považován za legitimní a často i nezbytný.

K zajímavému zdůvodnění přípustné délky uchování dat došel generální advokát ve zdůvodnění lhůty uchování dat – dle jeho subjektivního názoru lze dobu „měřenou na měsíce“, kterou lze považovat za přítomnost, oddělit od doby „měřené na roky“, kterou je nutné považovat za minulost. K uchování dat z minulosti nevidí žádný důvod, a proto za přiměřenou stanoví dobu jednoho roku.

Hlavním důvodem je zmapování věrného obrazu soukromé identity sledovaných osob. Kromě toho ale také viděl problematický samotný způsob regulace z následujících důvodů:

- není zde požadavek na uchování dat na serverech umístěných v EU,⁴⁵
- existuje zvýšené riziko použití údajů k protiprávním účelům,
- doba uchování dat může dosáhnout až 2 let, tedy směrnice je neslučitelná se zásadou proporcionality.

⁴⁵ Tato chybějící povinnost by mohla omezit dohled vnitrostátního orgánu.

4.10.3 Závěr stanoviska

Generální advokát prohlásil, že na další kategorie otázek již není nutné odpovídat a v závěru svého stanoviska se zaměřil na navrhované účinky konstatované neplatnosti.

Rozhodování bylo v zásadě mezi zachováním právní jistoty a odložení neplatností směrnice a na druhé straně nutnosti zrušit směrnici okamžitě z důvodu porušování základních práv a svobod. Generální advokát navrhl první možnost.

Soudní dvůr nebyl tímto stanoviskem generálního advokáta vázán a v prosinci 2013 začal soudní dvůr o dané věci rozhodovat (viz další kapitola).

Soudní dvůr tak rozhodl trochu jinak než v roce 2009 (kapitola 4.6 této práce) – v tomto sporu Irsko však šlo o volbu právního základu a nikoliv samotnou otázku lidských práv a svobod.

4.11 Zrušení směrnice č. 2006/24/ES

Po rozhodnutí generálního advokáta popsaném v minulé kapitole následovalo rozhodování Soudního dvora ve velkém senátu v čele s předsedou Vassiliem Skourisem.

Rozhodnutí Soudního dvora prohlásilo Směrnici č. 2006/24/ES, 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, za neplatnou.

Zdůvodnění bylo obdobné jako v případě rozhodnutí generálního advokáta. Šlo speciálně o tyto body:

- uchovávání údajů a znalosti četnosti komunikace, na jejichž základě lze vyvodit závěry o každodenních zvyklostech včetně denních přesunů, společenských vztazích apod.,

- skutečnost, že se uchovávají údaje, byť bez jejich obsahu, může mít dopad na užívání komunikačních systémů a tedy i na výkon svobody projevu zaručené v článku 11 Listiny základních práv a svobod EU,⁴⁶
- uchovávání údajů spolu s jejich zpřístupněním vnitrostátním orgánům se dotýká soukromého života a tedy práv zaručených článkem 7,⁴⁷
- směrnice byla zkoumána také s ohledem na článek č. 8 (zacházení s osobními údaji),
- zásah do základních práv se jeví jako velmi rozsáhlý a to, že k uchovávání a následném užití dochází bez informování účastníka může vyvolávat dojem, že jeho soukromí je pod neustálým dohledem,
- směrnice sama o sobě nestanoví žádná hmotněprávní či procesněprávní podmínky pro přístup vnitrostátních orgánů. Obdobně také nestanoví žádné kontroly, zda poskytovatelé zavedli dostatečná opatření pro zaručení bezpečnosti dat,
- směrnice nerozlišuje žádná pravidla pro stanovení lhůty uchovávání údajů (6-24 měsíců).

Zajímavé bylo stanovisko portugalské vlády, které konstatovalo, že existují i způsoby elektronické komunikace, které nespádají do působnosti této směrnice nebo které umožňují anonymní komunikaci – soud se s ním však neztotožnil a navíc vytváří otázku případné v jednom z cílů směrnice – vyšetřování kriminality a boji proti terorismu.

Na rozdíl od doporučení generálního advokáta zrušil směrnici s okamžitou platností od dubna 2014.

⁴⁶ Čl. 11 odst. 1 Listiny základních práv a svobod EU: „Každý člověk má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat či šířit informace bez zásahů státní moci a bez ohledu na hranice státu.“

⁴⁷ Každý člověk má právo na respektování svého soukromého a rodinného života, obydlí a korespondence či jiných druhů komunikace.

4.12 Vývoj v ČR po zrušení směrnice č. 2006/24/ES

Pirátská strana na základě zrušení směrnice zaslala vládě ČR výzvu, aby na základě zrušení směrnice předložila Ústavnímu soudu návrh na zrušení dotčených předpisů (tedy konkrétních paragrafů ZoEK). Odvolává se přitom na § 188 odst. 1 zákona č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů: *„Shledal-li mezinárodní soud, že zásahem orgánu veřejné moci byl porušen závazek, který pro Českou republiku vyplývá z mezinárodní smlouvy, zejména, že tímto zásahem bylo porušeno lidské právo nebo základní svoboda fyzické nebo právnické osoby, a jestliže takové porušení spočívá v platném právním předpisu, podá vláda Ústavnímu soudu návrh na zrušení takového právního předpisu nebo jeho jednotlivých ustanovení, pokud zrušení nebo změnu nemůže zajistit jiným způsobem. Ustanovení § 35 odst. 1 o nepřípustnosti návrhu na zahájení řízení ve věci, o níž již Ústavní soud rozhodl, se v tomto případě nepoužije.“*

Hlavní výtku generálního advokáta a SD EU – doba uchovávání dat počítaná na roky – však v českém zákoně nepředstavuje problém, protože počítá pouze se šesti měsíci.

Druhou část vyjádření Pirátské strany – Výzva poskytovatelům připojení, kterým radí nečekat na rozhodnutí ÚS a přestat uchovávat údaje již nyní – se jeví poměrně spornou, protože data jsou uchovávána na základě platného zákona (ZoEK) a nikoliv zrušené směrnice a operátoři by naopak porušovali zákon, pokud by tak přestali činit.

4.13 Rozhodnutí po zrušení směrnice č. 2006/24/ES v dalších zemích EU

Po zrušení směrnice zareagovalo mnoho evropských soudů – ne všechny však data retention ve své zemi zrušily.

4.13.1 Kde bylo data retention zrušeno

4.13.1.1 Slovensko

Prvním soudem, který o data retention rozhodoval po zrušení směrnice byl slovenský Ústavní soud. Návrh k němu byl podaný již v říjnu 2012 slovenskou neziskovou organizací EISi a podpořen 30 poslanci Slovenské národní rady.⁴⁸ Ústavní soud 23. dubna 2014 předběžně pozastavil povinnost uchovávání dat, nikoliv však možností jejich vyžadování od státu, která zůstává i nadále v platnosti.

4.13.1.2 Rakousko

V červnu 2014 prohlásil Ústavní soud data retention za protiústavní – konstatoval příliš závažné zásahy do lidských práv a článku 8 Evropské úmluvy o lidských právech.

Své rozhodnutí zdůvodnil kromě zásahů do lidských práv také nedostatkem bezpečnostních opatření ve skladování dat.

4.13.1.3 Rumunsko

V Rumunsku prodělala zákonná úprava podobný vývoj jako v České republice – po transpozici směrnice v roce 2008 prohlásil rumunský ústavní soud zákon č. 298/2008 za protiústavní v roce 2009. Po té, co Rumunsku hrozila žaloba Evropské komise pro neimplementování, vznikl nový zákon č. 82/2012 v roce 2012. V červenci 2014 však byl i tento zákon označen ústavním soudem za protiústavní.

4.13.1.4 Slovinsko

Slovinský ústavní soud v červenci 2014 také zrušil články 162-169 zákona odpovídající českému ZoEK týkající se data retention a to včetně vymazání nashromážděných dat po uveřejnění rozsudku. Důvodem byla doba uchovávání dat (8 měsíců pro internet a 14 měsíců pro telefonování) bez jejího odůvodnění, data nebyla omezena jen na vážné zločiny.

⁴⁸ European Information Society Institute

4.13.2 Kde data retention zůstává v platnosti

4.13.2.1 Dánsko

Naopak Dánsko je příkladem země, kde data retention pravděpodobně zůstane v platnosti i nadále. Dánský parlament se po zrušení směrnice obrátil na vládu s dotazem na dopady na dánský zákon – vláda ve své analýze došla k závěru, že data retention zůstává v platnosti.

Dánský zákon byl přijatý již v červnu 2002 (ačkoliv byla z důvodu technických omezení a také souladu s právem EU odložena účinnost až do roku 2007).

Data jsou uchovávána po dobu jednoho roku. Zvlášť závažný čin je zde definován jako zločin s možností odnětí svobody na dobu delší než 6 let.

Zvláštností místního zákona je neukládat informace o kompletní internetové komunikaci, ale „pouze“ o každém 500. paketu (vzhledem k množství takovýchto paketů jde o úsporu dat, ovšem stále vydatné sledování).⁴⁹

Dánsko se má však dalšímu osudu zákona o DR věnovat a je možné že při této příležitosti dojde ke změnám, ve kterých se projeví i rozhodnutí Soudního dvora.

4.13.2.2 Velká Británie

Podobně jako v Dánsku, i ve Velké Británii zůstává data retention v platnosti i po zrušení směrnice – v červenci 2014 prošel parlamentem během dvou dní zákon Data Retention and Investigatory Powers Bill se zdůvodněním, že zrychlený režim je nutný pro to, aby stát nepřišel o nasbíraná data z důvodu zrušení směrnice. Nová norma byla královnou podepsána 17. července 2014, s platností od následujícího dne.

⁴⁹ Paket = malá část dat, do které se dělí provoz v protokolu IP. Podrobnější informace jsou uvedeny v kapitole 5.1.1.5.

4.14 Další úprava související s data retention

4.14.1 Evidence počtu případů

Poskytovatelé služeb elektronických komunikací mají na základě § 97 odst. 10 ZoEK povinnost vést evidenci počtu případů, kde základě žádosti poskytl na provozní a lokalizační údaje, doby od zahájení sběrů údajů do doby jejich dožádání a počty případů, kde nemohli žádosti o poskytnutí údajů vyhovět.

Vyhláška ČTÚ 318/2010 Sb. stanoví detaily této povinnosti, resp. pouze specifikuje formu předávání dat – pomocí aplikace Elektronického sběru dat ČTÚ.

4.14.2 Čísla tísňového volání

Speciální pravidla pro předávání lokalizačních údajů stanoví vyhláška 238/2007 Sb. Tato vyhláška počítá s předáváním údajů pro účely tísňových linek, speciálně 112. Pro účely pevných linek jde o pravidelný export dat, ve kterém jsou údaje o geografické poloze linek, u mobilních telefonů pak jde o rozhraní (API) pro předání informace o aktuální poloze telefonu.⁵⁰

Vyhláška je podrobnějším rozpracováním § 33 Zákona o elektrických komunikacích.

4.14.3 Pátrání po osobách

Podle zákona č. 273/2008 Sb. o policii si může policie v souladu s § 68 vyžádat provozní a lokalizační údaje při pátrání po osobách a věcech, konkrétně:

- pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě,
- za účelem zjištění totožnosti osobnosti neznámé osoby či nalezené mrtvoly.

Útvar policie, jehož úkolem je boj s terorismem, také podle § 71 zákona o policii může žádat o provozní údaje (v takovém případě není vyžadováno schválení soudem).⁵¹

Pro rozsah a formu poskytovaných informací se použijí ustanovení ZoEK.

⁵⁰ API = Application Programming Interface.

⁵¹ Kromě toho také může policie dle § 71 žádat o údaje od bank a zdravotních pojišťoven.

4.14.4 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, z června 2014 upravuje povinnosti významných provozovatelů telekomunikačních sítí, významných informačních systémů. Konkrétně se týká spolupráce s těchto subjektů s Národním bezpečnostním úřadem (*NBÚ*) ohledně předcházení, řešení bezpečnostních incidentů či vyhlášení stavu kybernetického nebezpečí.⁵²

Zákon o kybernetické bezpečnosti novelizuje stávající Zákon o elektronických komunikacích v oblasti provozních údajů § 89, odst. 4: nově zavádí povinnost poskytovatelů poskytnout účastníkovi na jeho žádost jeho provozní údaje, pokud účastník nemohl v důsledku kybernetického bezpečnostního incidentu zprávu (hovor apod.) přijmout. Tyto údaje musí být poskytnuty do 3 dnů a v dále zpracovatelné formě.

⁵² S účinností od 1. ledna 2015.

5 Data retention v praxi

5.1 Rozsah ukládaných dat

Provozní data, která má poskytovatel povinnost ukládat, byla definována směrnicí č. 2006/24/ES v článku č. 5. Konkrétní technické parametry, které platí v ČR, jsou uvedeny ve vyhlášce 357/2012 Sb. (dříve 485/2005 Sb.).

Základní sítě, u kterých připadá ukládání dat v úvahu, jsou:

- pevná telefonní síť
- mobilní telefonní síť
- připojení k internetu.

5.1.1 Pevná telefonní síť (hovory)

Telefonní síť, ve které se nemění poloha a operátor zná totožnost svého zákazníka. Po dobu spojení hovoru je zákazníkovi přidělená část sítě a nemění se síťové prvky, kterými je hovor uskutečněn. Jako údaje, které mohou být ukládány, připadá v úvahu hlavně volající, volaný, zda došlo k uskutečnění hovoru a jeho doba.

5.1.2 Mobilní telefonní síť (hovory)

Mobilní síť je oproti pevné síti technicky složitější a klade větší nároky na ukládání provozních i lokalizačních dat.

Pro spojení hovoru se stejně jako v pevné síti používá telefonní číslo, ovšem v průběhu hovoru se mohou měnit síťové prvky, kterými hovor prochází (typicky při pohybu telefonujícího).

Síť musí navíc trvale sledovat polohu telefonu i v tzv. pohotovostním režimu, aby bylo možné spojit příchozí hovor či doručit SMS zprávu (kapitola 1).

Oproti pevné síti zde operátor také mnohem častěji nezná identitu zákazníka – pokud zákazník používá předplacenou kartu, je pouze na něm, zda poskytne své osobní údaje (pro marketingové účely).

5.1.3 Datová síť (připojení k Internetu)

Samotný Internet funguje na jiných principech než standardní telekomunikační síť – probíhá zde množství různých typů spojení a na rozdíl od telefonní sítě zde chybí kontrola, kudy jsou jaká data posílána. Přesto je však možné každé spojení sledovat a určit, ze kterého počítače bylo uskutečněno.

Připojení k internetu může být jak pevné (telefonní síť, pronajatá pevná linka), tak mobilní.

5.1.4 Provozní data v pevné telefonní síti – hlas

Tabulka 1: Provozní data ukládaná v pevné telefonní síti dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
Telefonní číslo volajícího ⁵³	Pro telefonní číslo se používá označení MSISDN ⁵⁴	§ 2/1a
Telefonní číslo volaného		§ 2/1a
Telefonní čísla, která se zúčastnila konferenčního hovoru	V případě, že šlo o konferenční hovor, tedy službu, při které je spojeno více účastníků – ačkoliv z pohledu telefonního zařízení jde o jeden hovor.	§ 2/1a
Identifikátor telefonní karty	U veřejných telefonních automatů	§ 2/1a
Datum a čas zahájení hovoru		§ 2/1b
Délka hovoru		§ 2/1c
Datum a čas odeslání SMS	SMS zprávy jsou dostupné i v pevné telefonní síti.	§ 2/1d
Typ telefonní služby	Rozdělení dle § 1/m: Hlasová služba Hlasová schránka Videohovor Přeložení, přesměrování či konferenční volání SMS	§ 2/1e
Stav komunikace	Zda došlo ke spojení hovoru	§ 2/1f
Doplňující údaje	§ 2/4: Cílová země či země původu u mezinárodních hovorů Přehled poskytovatelů, přes které byl směřovaný hovor	§ 2/1g
Jméno, příjmení a adresa zákazníka		§ 2/5

⁵³ Případně telefonní číslo odesílatele SMS.

⁵⁴ MSISDN = Mobile Subscriber Integrated Services Digital Network Number.

Destinace nebo kód země příchozího mezinárodního volání		§ 3/f
Kód provozovatele veřejné komunikační sítě nebo propojení		§ 3/f
Popis provozovatele neveřejné komunikační sítě		§ 3/f

Kromě těchto údajů cílených na konkrétního zákazníka má poskytovatel také povinnost uchovávat údaje:

- o veřejných telefonních automatech – jejich telefonní, evidenční číslo a jejich zeměpisnou polohu (§ 6a),
- o všech přístupových bodech s jejich označením a zeměpisnou polohou (§ 6e).

5.1.5 Provozní a lokalizační data v mobilní síti – hlas

Tabulka 2: Provozní a lokalizační data ukládaná v mobilní síti dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
Telefonní číslo volajícího ⁵⁵		§ 2/1a
Telefonní číslo volaného		§ 2/1a
Identifikátor IMSI	IMSI je jednoznačný celosvětově unikátní identifikátor zákazníka v mobilní síti. Jde o základní parametr z pohledu mobilní sítě (namísto MSISDN), zákazník však s tímto číslem standardně nepřichází do styku. ⁵⁶	§ 2/2a
Telefonní čísla, která se zúčastnila konferenčního hovoru		§ 2/1a
Datum a čas zahájení		§ 2/1b

⁵⁵ Případně telefonní číslo odesílatele SMS či MMS.

⁵⁶ IMSI = International Mobile Subscriber Identity.

hovoru		
Délka hovoru		§ 2/1c
Datum a čas odeslání SMS		§ 2/1d
Datum a čas odeslání MMS		§ 2/2c
Označení základnové stanice (BTS), přes kterou hovor začal		§ 2/2d
Základnová stanice, kde skončil		§ 2/2d
Identifikátor volajícího přístroje (IMEI) ⁵⁷	Výrobní číslo mobilního telefonu	§ 2/2b
Identifikátor volaného přístroje (IMEI)		§ 2/2b
Typ telefonní služby	Rozdělení dle § 1/m: Hlasová služba Hlasová schránka Videohovor Přeložení, přesměrování či konferenční volání SMS MMS	§ 2/1e
Stav komunikace	Zda došlo ke spojení hovoru	§ 2/1f
Doplňující údaje	Viz předchozí tabulka	§ 2/1g
Jméno, příjmení a adresa zákazníka		§ 2/5

Dále musí poskytovatel uchovávat informace o:

- všech základnových stanicích (BTS) a jejich zeměpisné poloze včetně označení, kam je daná stanice namířena – tzv. cellplan (§ 6b)
- údaje o vazbách mezi MSISDN (telefonní číslo), IMSI (identifikátor zákazníka v mobilní síti) a IMEI (výrobní číslo telefonu) – § 6c)
- datum, čas a označení základnové stanice, kde byla provedena aktivace předplacené karty (§ 6d)

5.1.6 Internet

Pro Internet je typické, že komunikace probíhá na více různých vrstvách a proto na ukládání údajů klade vyhláška větší nároky než na jiné typy sítí.

⁵⁷ IMEI = International Mobile Equipment Identity

Základní rozdělení je na vrstvě IP.⁵⁸ Tato vrstva se stará o doručení jednotlivých částí dat (paketů) a jejich správné nasměrování do konkrétního počítače (příp. serveru) a tato vrstva také řeší spolehlivost přenosu.

IP adresa je tak základní adresou, jde o obdobu telefonního čísla – skládá se ze 4 po sobě jdoucích čísel 0-255 (v nové verzi IP protokolu IPv6 jde o 8 hodnot oddělených dvojtečkou a používají se čtyřmístná čísla v šestnáctkové soustavě).

Síťové názvy (např. prf.cuni.cz) fungují jako alias, díky kterému si návštěvník nemusí pamatovat přesnou IP adresu (pro prf.cuni.cz jde o 195.113.8.11).

Dalším důležitým parametrem je vedle IP adresy i port.

Existence portů se využívá pro přesnější vymezení typu spojení a je možné si ho představit jako „podadresu“ v daném počítači. Například standardní internetový provoz v prohlížeči (HTTP) používá port 80, šifrovaný provoz HTTPS port 443, přenos souborů přes FTP⁵⁹ port 21 a podobně.

Konvence pro zápis je IP adresa:port, přístup pro web prf.cuni.cz tedy míří na adresu 195.113.8.11:80.

Každý paket může být přenášén jinou cestou (jinými částmi sítě, jinými síťovými prvky) a samotná IP vrstva tedy poskytuje „pokličku“, která zaručuje, že data budou přenesena, ovšem uživatelé (jejich programy) nemusí řešit kudy – proto se tyto sítě také označují jako sítě s přepojováním paketů. Samotné směrování pak probíhá díky nastavení pravidel a díky algoritmům na síťových prvcích. Síťové prvky jsou pak identifikovány tzv. MAC adresou.⁶⁰

⁵⁸ IP = Internet Protocol.

⁵⁹ FTP = File Transfer Protocol.

⁶⁰ MAC = Media Access Protocol.

Internet má také další vlastnost, která představuje problém pro data retention. Zatímco v tradičních telekomunikačních sítích se síť stará o spojení až do konkrétního zařízení (a to jak v pevné, tak v mobilní síti), u připojení k internetu v určitém místě končí síť poskytovatele a za ní už jde o síť zákazníka, jejíž provoz vidí operátor jako celek. Nemusí přitom jít o rozsáhlé firemní sítě, tato situace nastává tradičně u domácností – operátor neví, který konkrétní počítač z domácnosti byl připojen.

5.1.7 Síť elektronických komunikací s přepojováním paketů

Tabulka 3: Provozní data ukládaná v sítích s přepojováním paketů dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
Typ připojení		§ 2/3a
Telefonní číslo nebo označení uživatele		§ 2/3a
Identifikátor uživatelského účtu		§ 2/3a
Adresa MAC	Označení zařízení, resp. prvku řešícího přístup k síti	§ 2/3a
Datum a čas zahájení a ukončení připojení		§ 2/3a
Označení přístupového bodu u bezdrátového připojení		§ 2/3a
Adresa IP a číslo portu	Portem se rozumí číslo popisující typ služby	§ 2/3a
Jméno, příjmení a adresa zákazníka		§ 2/5

U připojení k Internetu s přepojováním paketů z mobilního připojení se navíc ukládají tyto informace:

Tabulka 4: Provozní data ukládaná v mobilních sítích s přepojováním paketů dle vyhlášky č. 357/2012 Sb. (doplnění tabulky 3)

Název	Popis	Vyhláška
Identifikátor mobilního zařízení	IMEI – viz mobilní síť	§ 2/3b
Označení základnové stanice, kde přenos začal, a kde skončil		

K překladu IP adres dochází v případě, že více zákazníků vystupuje pod jednou IP adresou. Tato situace je typická u mobilních operátorů, kdy více zákazníků přistupuje k internetu, ovšem poskytovatel nemá dost IP adres na to, aby pro každý mobilní telefon zajistil jednu IP adresu. Pod jednou IP adresou tak může během jedné minuty být mnoho různých telefonů/zákazníků.

Vyhláška v odstavci § 2/3f pamatuje i na tuto možnost překladu IP adres a požaduje ukládání identifikačních údajů k překladu.

Oproti tomu pevná připojení (typicky ADSL, kabelová televize či pevné připojení) mají většinou stálou IP adresu, která se v čase nemění (nebo například jen při novém navazování spojení).

U přístupu ke schránce (stahování přijatých zpráv) elektronické pošty se ukládá:⁶¹

Tabulka 5: Provozní data ukládaná u přístupu ke schránce dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
IP adresa a port zdrojového počítače		§ 3/3c
Identifikátor uživatelského účtu		§ 3/3c
Datum a čas zahájení a ukončení připojení ke schránce		§ 3/3c
Identifikátor protokolu	POP3 či IMAP	§ 3/3c

⁶¹ V případě protokolu IMAP i synchronizace všech složek včetně odeslané pošty

U odesílání zpráv elektronické pošty pomocí protokolu SMTP se ukládá:

Tabulka 6: Provozní data ukládaná při odesílání elektronické pošty dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
IP adresa a port zdrojového a cíle přenášené zprávy		§ 3/3d
Datum a čas odesílání zprávy		§ 3/3d
Adresy odesílatele a příjemců		§ 3/3d
Stav přenosu zprávy	Odesláno/neodesláno	§ 3/3d
Identifikátor protokolu	SMTP	§ 3/3d
Jméno, příjmení a adresa zákazníka		§ 2/5

Tato data však mají smysl pouze v případě, že uživatel používá e-mailového klienta (např. Microsoft Outlook, Mozilla Thunderbird či aplikaci v mobilním telefonu).

Webové rozhraní, přes které velká část uživatelů používá e-mail, se v takovém případě v záznamu jeho provozu neprojeví resp. ne jako příjem a odesílání e-mailu.

Další odstavce vyhlášky řeší poskytování dat o IP telefonii (VoIP).⁶² IP telefonie je způsob telefonního spojení, při kterém hovor (či jeho část) probíhá po IP síti (internetu). Ačkoliv se při vzniku této technologie počítalo s tím, že se IP adresy budou používat namísto telefonních čísel, k takovému využití prakticky nedošlo. IP telefonie se typicky používá ve firmách pro spojení mezi jednotlivými pobočkami – i zde se ale používají tradiční telefonní čísla, tedy uživatel nepozná rozdíl oproti tradičnímu telefonu. Po standardních telefonních linkách také většinou hovory odcházejí ven z ústředny.

⁶² Voice over IP

Dalším využitím IP telefonie byla dříve možnost volat do zahraničí levněji tím, že zákazník pomocí speciální předvolby zvolil směřování části hovoru po internetu – jinak šlo ale z jeho pohledu o standardní telefonní hovor.⁶³

Z dnešního pohledu jsou mnohem častěji využívány aplikace jako Skype (ať už pro hovory mezi uživateli sítě nebo pro volání do standardní telefonní sítě - PSTN) či aplikace (VoIP klienti) do mobilních telefonů (Viber, WhatsApp).⁶⁴

V těchto případech se ale nepoužije část vyhlášky řešící IP telefonii, ale standardní logování internetového provozu.

Pokud ale dojde opravdu na ukládání dat dle vyhlášky o IP telefonii, použijí se následující data:

Tabulka 7: Provozní data ukládaná u IP telefonie dle vyhlášky č. 357/2012 Sb.

Název	Popis	Vyhláška
IP adresa a port zdrojového a cílového zařízení		§ 3/3e
Transportní protokol		§ 3/3e
Datum a čas zahájení a ukončení komunikace		§ 3/3e
Destinace nebo kód země původu volání u příchozích mezinárodních volání		§ 3/4
Kód provozovatele veřejné komunikační sítě nebo telefonní služby		§ 3/4
Název poskytovatele zajišťující neveřejnou komunikační síť a její identifikaci		§ 3/4
Jméno, příjmení a adresa zákazníka		§ 2/5

⁶³ Šlo například o EuroTel NetCall-55 či Paegas InternetCall.

⁶⁴ PSTN = Public Switched Telephone Network

5.2 Postup při vydávání dat

Existují dva nejčastější způsoby, podle kterých policie žádá o poskytnutí provozních a lokalizačních údajů:

- policie má identifikaci konkrétního uživatele (jeho telefonní číslo mobilní či pevné linky, IP adresu, výrobní číslo mobilního telefonu apod.)
- policie nemá identifikaci konkrétního uživatele, ale má např. údaj o tom, kde se uživatel (podezřelý) pohyboval a žádá o výpis údajů k jednotlivým BTS stanicím.

Interní postup policie je upraven Závazným pokynem policejního prezidenta č. 186/2011, který však není veřejně dostupný.

Policie se prostřednictvím státního zástupce obrátí s žádostí o přikázání poskytnutí provozních údajů na soud (v případě fáze řízení před soudem nařídí přímo předseda senátu). S tímto příkazem soudu se policista obrátí na Útvar zvláštních činností policie, který zprostředkuje předání od poskytovatele (operátora). Jedna z expozitur⁶⁵ Útvaru si pak prostřednictvím Centra informačních systémů vyžádá kompletní výpis. Prostřednictvím policejního intranetu je pak výpis dodán policistovi, který si údaje vyžádal. Obsah je přístupný pod heslem, které zvolil policista při podání žádosti.

Může také nastat situace, kdy by policista tento postup obešel a žádal přímo poskytovatele na základě § 8 TrŘ.⁶⁶ Takto získané důvody by však u soudu mohly být považovány za neplatné z důvodu získání nezákonnou cestou dle § 89 odst. 3 ZoEK – úprava v ZoEK představuje v tomto případě *lex specialis*.

⁶⁵ Expozitura je oddělení Útvaru – po republice jich je 7 – konkrétně v Praze, Brně, Plzni, Českých Budějovicích, Hradci Králové, Ostravě a Ústí nad Labem.

⁶⁶ Zákon č. 141/1961 Sb., trestní řád, § 8: „*Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů....*“

5.3 Náklady

Úhradu nákladů poskytovatelům dat řeší vyhláška č. 462/2013 Sb. vydávaná Českým telekomunikačním úřadem (ČTÚ).⁶⁷

Sazby jsou odstupňovány podle doby, za kterou jsou data poskytována a také se rozlišuje standardizovaná stížnost (kterou lze vyřídit automaticky) a ostatní žádosti. V případě standardizovaných žádostí se pohybují ceny v řádech desítek korun, u ostatních žádostí v řádech stokorun (vždy pod 1 000 Kč).

5.4 Problémy na straně soudů

V souvislosti s poskytováním dat a jejich schvalováním soudy se stihlo objevit již několik problémů.

Například při kontrole soudců Okresního soudu v Děčíně došlo Ministerstvo spravedlnosti k závěru, že soudci schvalovali žádosti pouze formálně – konkrétním příkladem byla žádost od policisty, který v roce 2009 a 2010 dostal souhlas se sledováním padesáti čísel, mezi nimiž byl předseda ÚS, prezidentův kancléř, manažer ČEZu či novináři MF Dnes a to pod záminkami jako prověřování obchodu s bílým masem.

Z následné kontroly podobných případů vyplynulo, že osm soudců děčínského soudu vyhovělo v 18 případech žádostem, aniž by bylo jejich rozhodnutí dostatečně odůvodněné.

Ministr spravedlnosti podal na soudce kárné žaloby. Následná kontrola dalších čtyř soudů neukázala jiná pochybení.

Nejvyšší správní soud v březnu 2012 rozhodl ve prospěch předsedy děčínského soudu s tím, že šlo o selhání daného policisty a soud neměl šanci to odhalit. Policista

⁶⁷ Plný název vyhlášky zní: Vyhláška o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby.

byl obviněn pro přečin zneužití pravomoci úřední osoby. Podobně byla také v jiném případě obviněná kriminalistka, která si měla opatřovat výpisy hovorů bezpečnostní agentury.

5.5 Poskytování shromážděných údajů zákazníkům

Stále poměrně nevyjasněnou oblastí zůstává poskytování provozních a lokalizačních údajů zákazníkům, kterých jsou ukládány. Do nedávna byly všechny podobné žádosti směřované na jednotlivé poskytovatele zamítány, neboť ZoEK vůbec nepočítá s možností, že by tyto údaje byly poskytovány koncovým uživatelům.

5.5.1 Osobní údaje vs. provozní údaje

Na tomto místě je vhodné zmínit otázku, nakolik zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ), zasahuje do data retention, neboť tento zákon subjektům údajů umožňuje zjistit osobní údaje, které o něm jsou uchovávány.⁶⁸

Samotná provozní data definici osobního údaje v § 4 ZOOÚ splňují („*Pro účely tohoto zákona se rozumí (...) osobním údajem jakákoliv informace týkající se určeného nebo určitého subjektu údajů...*“).

Ustanovení § 3 odst. 6 tohoto zákona však stanoví, že osobní údaje zpracovávané *pro předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů* (písmeno d) mají zvláštní režim, díky kterému se na tyto údaje nevztahují některé z povinností pro správce (§ 5) a hlavně povinnosti dle § 11 (povinnost informovat subjekt údajů, poučení o dobrovolnosti poskytnutí apod.) a dle § 12 (poskytování údajů). Tato otázka byla následně upřesněna stanoviskem Úřadu pro ochranu osobních údajů (ÚOOÚ).

5.5.2 Konkrétní případy (SRN a ČR)

V Německu se v roce 2009 podařilo politikovi Malte Spitzovi získat od svého operátora provozní data – po několika žádostech a následné žalobě proti Deutsche Telekomu mu byla data poskytnuta. Nikoliv z rozhodnutí soudu, ale na základě mimosoudní dohody. Spitz se spolupracovníky připravil vizualizaci, díky které znázornil veřejnosti, jaký dopad může uchovávání dat mít a otevřel debatu nad tímto tématem.

⁶⁸ Subjektem údajů je v tomto případě zákazník.

V ČR podobně jednal Jan Cibulka, který si začátkem roku 2013 vyžádal data od českého T-Mobile. O data žádal na základě § 12 ZOOÚ.⁶⁹

T-Mobile se obrátil s žádostí o stanovisko k aplikaci § 12 zmiňovaného zákona v případě zpracování provozních a lokalizačních údajů na ÚOOÚ.

ÚOOÚ se ve svém stanovisku UOOU-00159/13-2 vyjádřil tak, že výjimky stanovené zákonem č. 101/2000 Sb. v § 12 (předcházení trestné činnosti) se paušálně nepoužijí na provozní data.

Argumentuje přitom tím, že *„nelze data retention považovat bez dalšího za zpracování, které je nezbytné pro předcházení, vyhledávání a odhalování trestné činnosti, a to přestože nelze zpochybnit, že těmto cílům uchování provozních a lokalizačních údajů slouží.“*⁷⁰

Dále argumentuje nutností, aby se jednotlivci mohli domáhat efektivní kontroly a ochrany svých dat, a tedy aby každý mohl zjistit, v jakém rozsahu a za jak dlouhé období jsou o něm u správce (poskytovatele) data uchovávána.

V závěru tedy ÚOOÚ konstatuje povinnost T-Mobilu poskytnout požadovaná data a zmiňuje, že výjimka dle § 3/6d by se vztahovala **pouze na data, která již byla poskytnuta oprávněným orgánům**, a která tedy naplňují účel předcházení (vyšetřování...) trestné činnosti.

V praxi by však doslovné dodržování této podmínky bylo nesmyslné. Poskytovatel by musel vymazat (nebo si nějakým způsobem speciálně označovat) údaje, které již byly poskytnuty oprávněným orgánům, protože poskytnutím takto „profiltrovaných“ údajů by zvýhodňoval podezřelého.

Všichni tři čeští mobilní operátoři již začali poskytovat provozní a lokalizační data zákazníkům.

⁶⁹ Ve znění: *„Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.“*

⁷⁰ Stanovisko UOOU-00159/13-2

5.5.3 T-Mobile Czech Republic a. s.

T-Mobile poskytne výpis údajů pouze zákazníkovi se smlouvou (tzv. *postpaid*) po prokázání, že jde o jeho číslo. Zákazník musí splnit podmínku, že má na smlouvě pouze jedno telefonní číslo – kdyby jich měl více, neposkytne data k žádné kartě (kvůli ochraně soukromí dalších osob).

T-Mobile neposkytne data o zákazníkovi používajícím předplacenou kartu (*prepaid*, služby s marketingovými názvy Twist a Kaktus), jelikož tato karta je anonymní.⁷¹

Cena za poskytnutí údajů je dle ceníku 1700 Kč.

5.5.4 O2 Czech Republic a. s.

O2 poskytování provozních dat ve svém ceníku ani v prohlášení o ochraně soukromí neuvádí, dle vyjádření O2 v článku Jiřího Peterky na zpravodajském serveru Lupa.cz umožňuje O2 tuto službu za cenu 1600 Kč.⁷²

5.5.5 Vodafone Czech Republic a. s.

Vodafone podobně jako ostatní operátoři nechtěl provozní údaje subjektům poskytovat a v odpovědi na dotaz autora této práce odpověděl pouze, že všechny žádosti o poskytnutí údajů vyřizuje v souladu s relevantními předpisy, nakonec ale stejně jako O2 a T-Mobile zařadil poskytnutí provozních dat do svého ceníku za 1 667 Kč.⁷³

⁷¹ Případná registrace v podobě vyplnění údajů pro účely marketingu nemá srovnatelnou váhu jako údaje ve standardní smlouvě uzavřené na základě osobních dokladů.

⁷² PETERKA, JIŘÍ Chcete své provozní a lokalizační údaje? Připravte si nejméně 1600 Kč *Lupa.cz* [online] 2014-08-11 [cit. 2014-11-25] Dostupné z <http://www.lupa.cz/clanky/chcete-sve-provozni-a-lokalizacni-udaje-pripravte-si-nejmene-1600-kc/>

⁷³ Příklad odmítavého postoje Vodafone ČR z 3. 12. 2013 na oficiálním kanálu společnosti na sociální síti Twitter (a související v konverzaci) Dostupné z:

https://twitter.com/vodafone_cz/status/407929564338610176

Skutečné počty žádostí o poskytnutí dat se ale například u T-Mobile pohybují pouze v jednotkách.

5.6 Poskytování údajů kvůli vyúčtování služeb

K velice zajímavému rozhodnutí, které se dotýká data retention, dospěl v srpnu 2013 Nejvyšší soud. Šlo o rozhodnutí sp. zn. 21 Cdo 2058/2012 z 27. srpna 2013.

Zpočátku šlo o poměrně standardní spor mezi zákazníkem a společností T-Mobile, ve které zákazník v roce 2008 reklamoval výši telefonního účtu, která se nepohybovala kolem standardních 1 000 Kč – operátor naúčtoval uživateli 45 tisíc Kč, přičemž 37 tisíc Kč bylo účtováno za datové přenosy.

Zákazník účet nejprve standardně reklamoval u svého operátora, následně podal námitku k ČTÚ, který účet snížil na 1 300 Kč. Důvodem, proč ČTÚ částku snížil, byla skutečnost, že T-Mobile nepředložil jako důkaz provozní údaje, konkrétně URL adresy webových stránek, které měl účastník navštívit. Ze stejného důvodu pak také předseda Rady ČTÚ v červnu 2009 zamítl rozklad.

V následné žalobě v červenci 2009 u Okresního soudu v Jičíně se operátor domáhal zrušení dřívějších rozhodnutí, a to z toho důvodu, že účtování datových služeb se provádí na základě množství přenesených dat a nikoliv konkrétních navštívených adres. Tato žaloba byla Okresním soudem v dubnu 2010 zamítnuta. Operátor měl podle názoru soudu uchovávat provozní údaje do doby, kdy je možné vyúčtování právně napadnout a tím, že seznam URL (či jiné provozní údaje, které by dokázaly obsah zprávy) neměl, se měl sám připravit o důkaz.

Citace z rozsudku Okresního soudu: *„Neztotožnil se s názorem žalobce, že poskytnutí služeb účastníku je dostatečně prokázáno vyúčtováním služeb a podrobným výpisem hovorů a připojení účastníka, neboť výpis hovorů a připojení i vyúčtování služeb jsou podle názoru soudu prvního stupně pouze „dokladem o tom, co poskytovatel služby elektronických komunikací naměřil a zaznamenal svými přístroji a co následně vyúčtoval“, a žalobcem tvrzený objem dat i časový údaj o trvání připojení jsou pouze „abstraktním číselným údajem“, který nemá s ohledem na povahu poskytované služby,*

spočívající v přenosu signálů po sítích elektronických komunikací, „v ničem reálném svůj podklad“ a který je plně závislý na správnosti měření přístroje, který zaznamenává telekomunikační provoz.

Naproti tomu URL (řetězec znaků s definovanou strukturou sloužící k přesné specifikaci umístění zdrojů informací na internetu, který definuje doménovou adresu serveru, umístění zdroje na serveru a protokol, kterým je možné zdroj zpřístupnit) je „přínejmenším“ důkazním prostředkem, který může poskytnout informaci o tom, zda vůbec a jakým způsobem byla datová služba užita, popřípadě zda byla užita řádně či zda byla zneužita třetí osobou.“⁷⁴

Soud došel k názoru, že dle § 64 odst. 1 ZoEK je důkazní břemeno v případě sporu o vyúčtování na straně poskytovatele a (citace z rozsudku): *„Z takto vymezeného břemene tvrzení a důkazního břemene vyplývá, že osobě poskytující služby elektronických komunikací nestačí k úspěchu ve sporu s účastníkem, popřípadě uživatelem, o úhradu ceny za poskytnuté datové služby tvrdit a prokazovat, jaký byl jí naměřený objem dat přenesených v průběhu poskytování datových služeb účastníku (uživateli), nýbrž že **tato osoba musí – má-li mít ve sporu úspěch – tvrdit a prokázat též to, co bylo obsahem poskytnuté datové služby (jaká data účastník, popřípadě uživatel prostřednictvím datové služby obdržel).**“⁷⁵*

Následné odvolání u Krajského soudu v Hradci králové v prosinci 2010 potvrdilo rozsudek Okresního soudu – soud zde konstatoval, že URL nejsou jediným způsobem, jak dokázat množství přenesených dat – poskytovatel však nedodal ani žádný jiný údaj (např. provozní údaje dle ZoEK, aniž by došlo k narušení čl. 10 Listiny základních práv a svobod), který by naznačoval množství přenesených dat.

⁷⁴ Okresní soud v Jičíně, rozsudek č. 10 C 67/2009-57 z 26. dubna 2010

⁷⁵ § 64 odst. 1 zní: *„Účastník, který je koncovým uživatelem, popřípadě uživatel veřejně dostupné služby elektronických komunikací, je povinen uhradit za poskytnutou službu cenu ve výši platné v době poskytnutí této služby.“*

Proti tomuto rozsudku podal operátor dovolání – opět namítal především skutečnost, že není oprávněn uchovávat informace o obsahu přenášených dat pro potřeby prostého vyúčtování a URL není provozním údajem, který dle ZoEK má uchovávat. (Dle vyhlášky 485/2005 Sb., ani aktuálně platné 357/2012 Sb. URL do povinně uchovávaných údajů pro potřeby PČR nepatří.)⁷⁶

Nejvyšší soud uznal přípustnost dovolání a konstatoval potřebu rozhodnutí významné právní otázky a to důkazní povinnosti poskytovatele ve sporu o ceně vyúčtování služeb. Nejvyšší soud se ztotožnil s rozhodnutím odvolacího soudu.

Na tomto rozsudku není zajímavé ani tak samotné rozhodnutí ve věci reklamace (může se zdát pochopitelné, že se ČTÚ i soudy zastaly zákazníka, který by např. v případě poruchy zařízení na straně operátora neměl žádným způsobem možnost prokázání opaku), ovšem samotný požadavek Úřadu a soudů o poskytnutí URL či jiných provozních údajů, pomocí kterých by šlo zjistit obsah zprávy.

Kromě toho, že zjišťování URL je velkým zásahem do soukromí, který je svým charakterem srovnatelný spíše s odposlechem,⁷⁷ pravděpodobně by navíc v dané situaci ani nic neprokázal, protože takto velké množství dat by mohlo odpovídat i jinému typu provozu (P2P, velký e-mail apod.), ve kterém se URL nepoužívají – to by však prokázaly standardní provozní údaje dle vyhlášky, kde by se takový záznam projevil.⁷⁸

Požadavek na alespoň naznačení obsahu komunikace je v rozporu s § 89 ZoEK, který zajišťuje důvěrnost obsahu zpráv (*„Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví*

⁷⁶ A dalších oprávněných subjektů

⁷⁷ Kromě zjištění jména serveru, na který návštěvník přistupoval, lze z URL vyčíst i například, co zde vyhledával.

⁷⁸ P2P = Peer to peer, systémy na sdílení souborů mezi jednotlivými účastníky.

jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti.“).

K podobnému názoru dospěla také společnost O2 – URL považuje za údaj, který nejenom, že jednoznačně nedokazuje množství přenesených dat, ale také ho považuje za součást obsahu zprávy.⁷⁹

5.7 Čestnost předávání dat státním orgánům

Operátoři na základě povinnosti stanovené ZoEK a následně vyhláškou č. 318/2010 Sb. předávají ČTÚ úřadu každoročně počty případů, kdy byla data vyžádána.

ČTÚ 20. března 2014 na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, tato data zveřejnil.⁸⁰

Při interpretaci výsledků došlo k následujícím úpravám:

- Od roku 2010 došlo k zpřesnění údajů o internetovém provozu – zatímco dříve byly poskytovány údaje „o internetu“, od 2010 se ve formuláři dělí na internet a přístup k e-mailům a dále pak přenos e-mailů. Údaje byly započteny jako internet z důvodu porovnatelnosti s předchozími roky.
- Obdobně od roku 2010 se vykazuje IP telefonie. Byla započtena jako pevná síť.

5.7.1 Počty vyžádání dat

Mezi roky 2008 a 2013 došlo celkem k 1 119 198 žádostí o vydání dat (dle informací ČTÚ).

Z toho v 1 062 588 (95 %) bylo žádostem vyhověno a data poskytnuta.

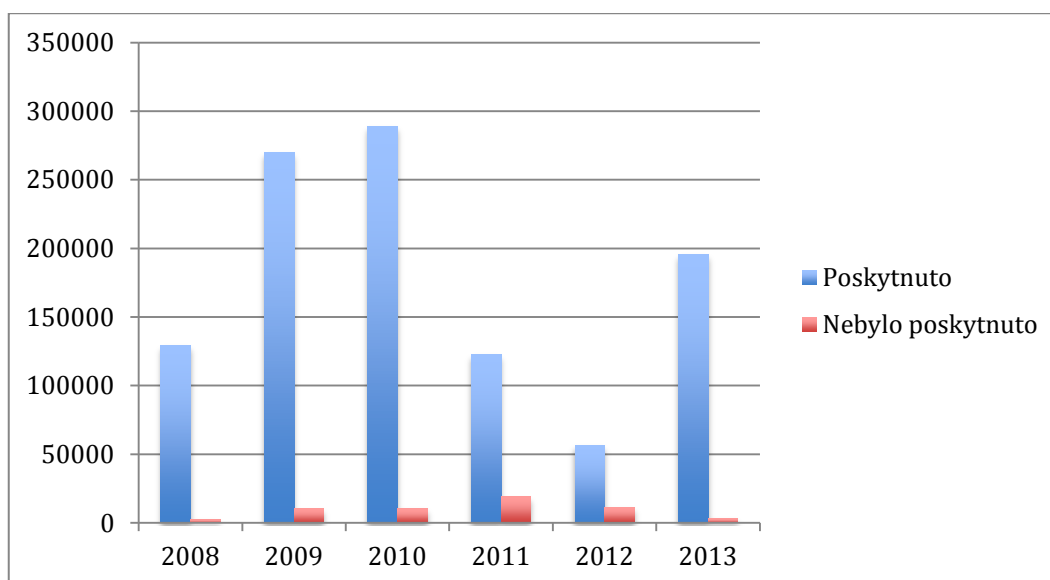
⁷⁹ Komplettní text vyjádření je k nalezení v příloze 1 této práce.

⁸⁰ ČTÚ, Počet případů provozních a lokalizačních údajů, dostupné online: http://www.ctu.cz/cs/download/ostatni/2014/informace_na_zadost-oldrich_kuzilek-06_03_2014-cj_9209_2014-604_e-mail.pdf z 6. března 2014

Na následujících datech je také vidět dopad nálezů ÚS, kdy v od 1. 4. 2011 do 1. 10. 2012 neplatila ustanovení o data retention.

Tabulka 8: Počty poskytnutých a neposkytnutých provozních údajů v letech 2008-2013

rok	žádostí	poskytnuto	nebylo poskytnuto	% neposkytnutých
2008	131 560	129 070	2 490	2 %
2009	280 271	269 825	10 446	4 %
2010	299 363	289 169	10 194	3 %
2011	141 531	122 685	18 846	13 %
2012	67 651	56 335	11 316	17 %
2013	198 822	195 504	3 318	2 %



5.7.2 Počty úkonů

Pro porovnání se statistikami ČTÚ je vhodné zmínit i data od Policejního prezidia ČR. Dle analýzy odposlechů (která uvádí také údaje o výpisech o uskutečněném telekomunikačním provozu, tedy data retention) z roku 2013 došlo k 54 560 vyžádání dat.⁸¹ Na první pohled zjevný nepoměr s daty ČTÚ je způsobený

⁸¹ Policejní prezidium České republiky, Úřad služby kriminální policie a vyšetřování, Analýza odposlechů a záznamu telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2013 z 6. června 2014, PPR-102-31/ČJ-2014-990390

jinou metodikou.⁸² Z analýzy také vyplývá, že téměř 96 % žádostí bylo na základě příkazu soudce – tedy 4 % se souhlasem sledované osoby.

5.7.3 Druh komunikace (poskytnutá data)

Mobilní síť je nejčastějším typem komunikace, o jejichž data je žádáno.

Z celkového počtu 1 062 588 poskytnutých dat tvoří:

- mobilní síť 953 205 (90 %),
 - pevná síť 89 494 (8 %),
 - internet 19 889 (2 %)
- vyhověných žádostí.⁸³

V případě mobilních telefonů byly tři čtvrtiny žádostí výpisy na buňky (tedy kdo se pohyboval v signálu dané stanice) a jedna čtvrtina na konkrétní mobilní telefony.⁸⁴

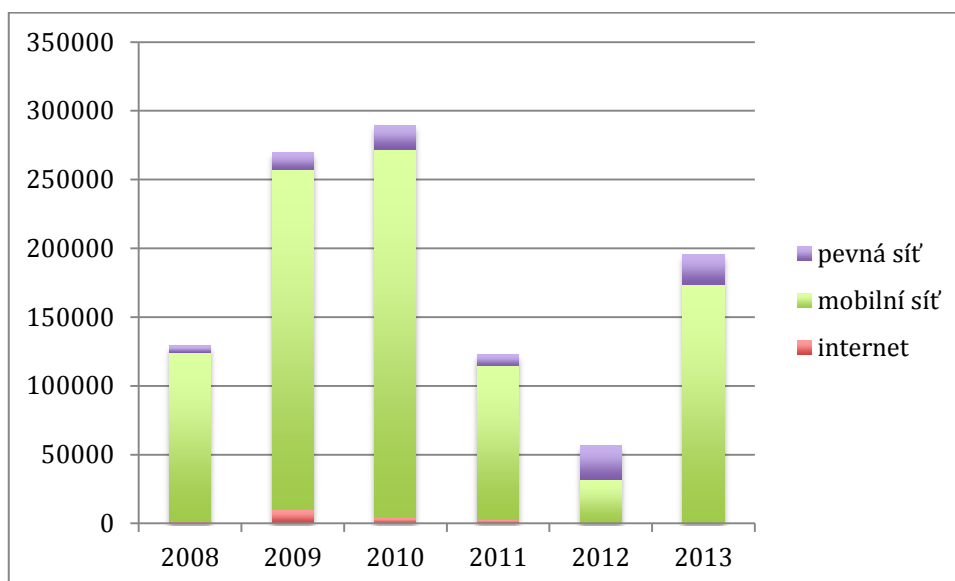
⁸² Hlavní rozdíl je v tom, že policie eviduje každou žádost všem operátorům jako jednu, zatímco ČTÚ za každého operátora. Detailnější informace naleznete ve zmiňované analýze v kapitole 4.5.1.

⁸³ Data ČTÚ

⁸⁴ Analýza policejního prezidia – viz výše. Z důvodu porovnávání odlišných metodik nejsou data uvedena s přesností na procenta, případný zájemce je však může najít ve zmiňované analýze na konci kapitoly 4.5.1.

Tabulka 9: Druhy komunikace v poskytnutých provozních datech v letech 2008-2013

rok	internet	mobilní síť	pevná síť
2008	1 454	122 764	4 852
2009	9 983	246 933	12 909
2010	4 327	267 820	17 022
2011	2 740	111 759	8 186
2012	733	30 842	24 760
2013	652	173 087	21 765



5.7.4 Stáří poskytnutých dat

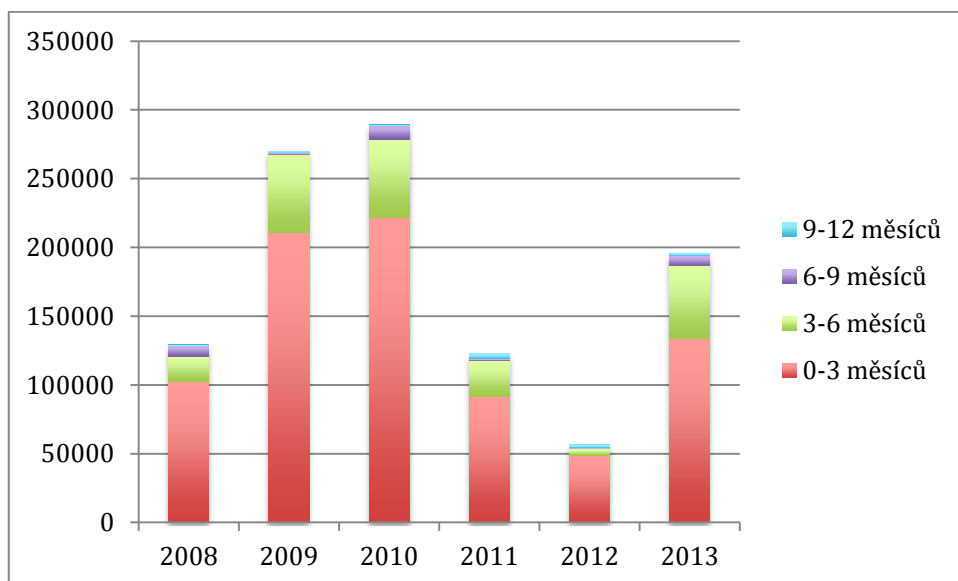
Nejčastěji poskytovaná data mají staří menší než 3 měsíce (doba, která uplynula od zahájení ukládání dat k jejich poskytnutí).

- 0-3 měsíců tvoří 809 294 (76 %)
- 3-6 měsíců 215 998 (20 %)
- 6-9 měsíců 28 202 (3 %)
- 9-12 měsíců 9 094 (1 %)

případů.

Tabulka 10: Stáří poskytnutých provozních údajů v letech 2008-2013

rok	0-3 měsíců	3-6 měsíců	6-9 měsíců	9-12 měsíců
2008	102 638	18 341	7 798	293
2009	210 908	56 559	1 380	978
2010	221 549	57 162	9 964	494
2011	91 497	26 408	994	3 786
2012	48 972	4 539	720	2 104
2013	133 730	52 989	7 346	1 439



5.8 Statistiky trestné činnosti

Následující data pocházejí ze statistik Ministerstva vnitra.⁸⁵

Tabulka 11: Počty zjištěných a objasněných trestných činů 2008-2013

rok	zjištěných TČ	objasněných TČ	% objasněných
2008	343 799	127 906	37 %
2009	332 829	127 604	38 %
2010	313 387	117 685	38 %
2011	317 177	122 238	39 %
2012	304 528	120 168	39 %
2013	325 366	129 181	40 %

⁸⁵ Ministerstvo vnitra ČR, Statistiky kriminality, dostupné online: <http://www.mvcr.cz/clanek/statistiky-kriminality.aspx>



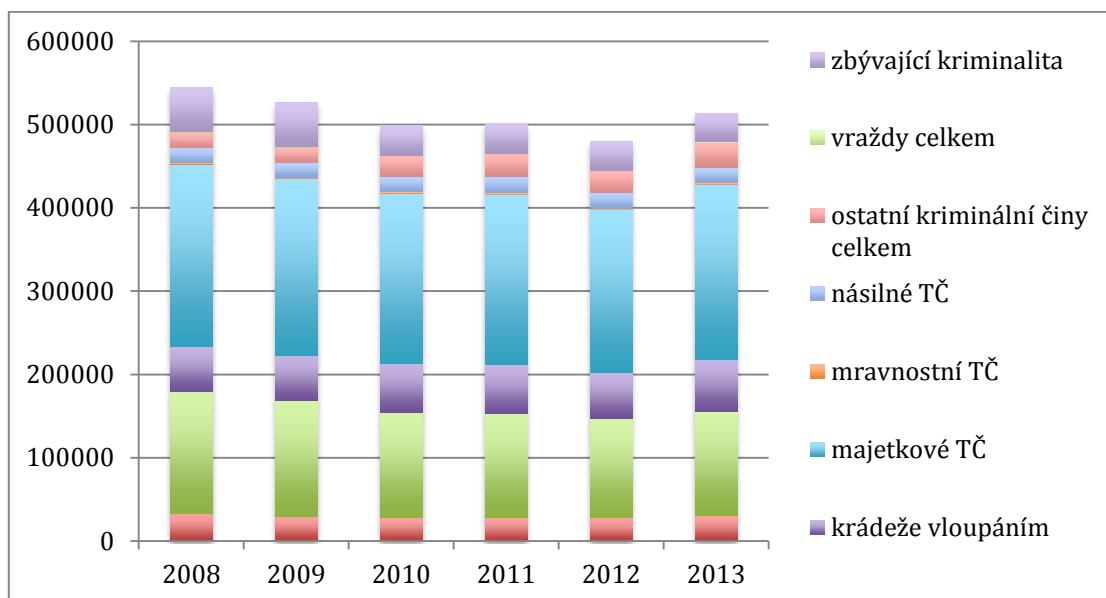
5.8.1 Typy trestné činnosti (zjištěné trestné činy)

Dělení trestných činů vychází z metodiky MV ČR. Jednotlivé skupiny trestných činů nejsou vždy disjunktní, tudíž součet jednotlivých skupin TČ neodpovídá součtu všech trestných činů na území České republiky za daný rok.

Konkrétní přehledy skutkových podstav lze najít v příložených souborech, ze kterých byla data čerpána.

Tabulka 12: Skupiny trestných činů zjištěných v letech 2008-2013

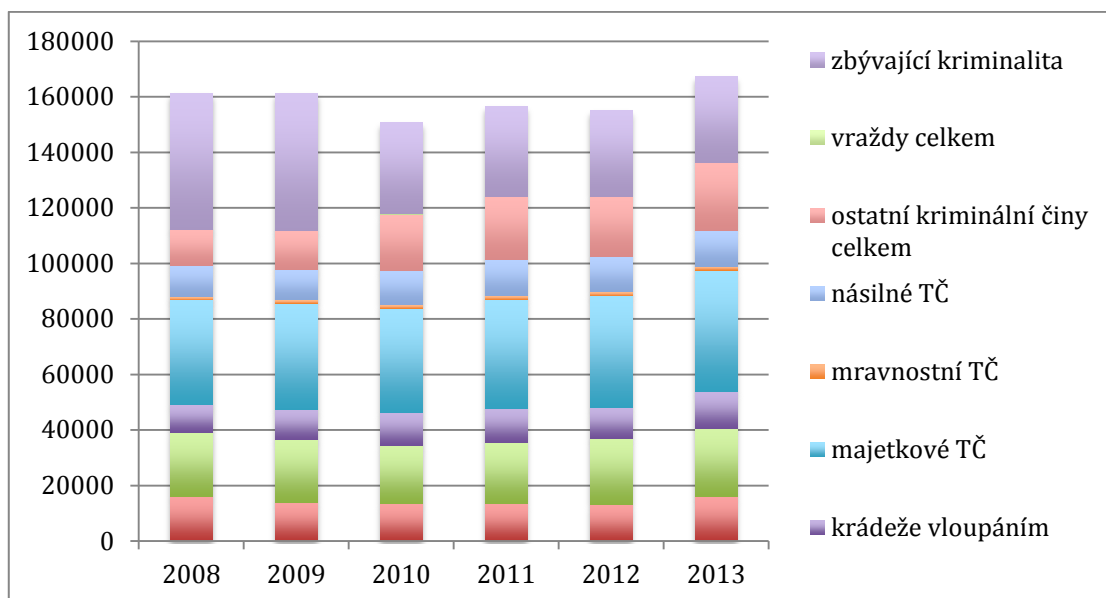
skupina TČ	2008	2009	2010	2011	2012	2013
hospodářské činy	32 474	29 774	28 371	28 216	27 633	30 376
krádeže prosté	147 292	138 369	126 311	124 274	119 367	125 573
krádeže vloupáním	53 381	54 858	58 758	59 672	55 554	62 384
majetkové TČ	219 347	212 168	203 717	203 675	194 970	209 351
mravnostní TČ	1 680	1 730	1 811	2 086	1 981	2 109
násilné TČ	17 875	16 887	18 073	19 409	18 358	18 689
ostatní kriminální činy celkem	18 861	19 190	25 437	27 787	27 140	30 316
vraždy celkem	202	181	173	173	188	182
zbývající kriminalita	53 524	53 056	35 960	35 984	34 434	34 522



5.8.2 Typy trestné činnosti (objasněné trestné činy)

Tabulka 13: Skupiny trestných činů objasněných v letech 2008-2013

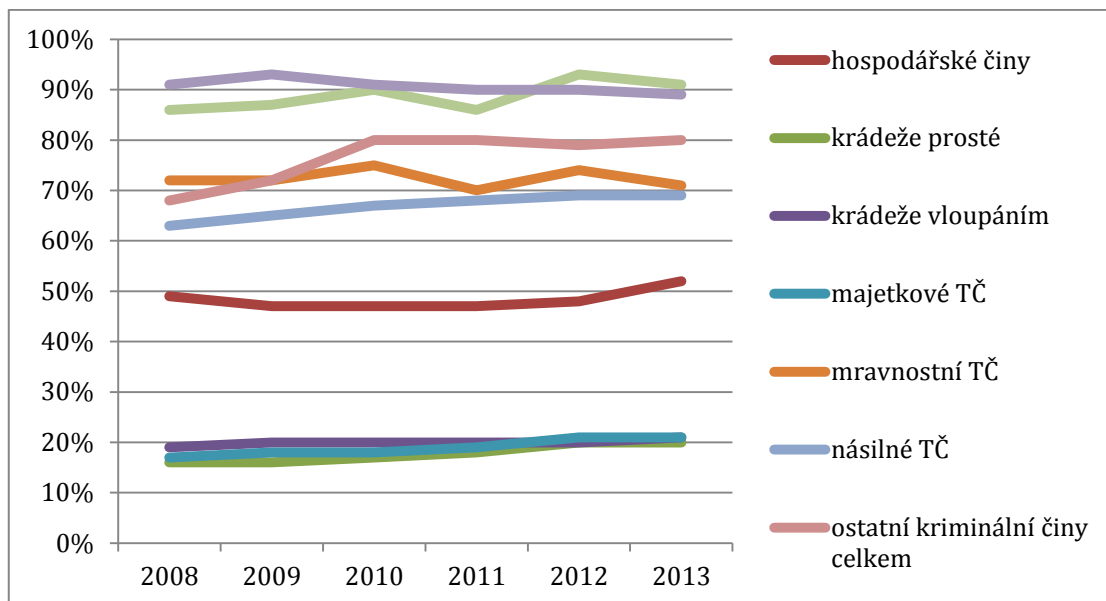
skupina TČ	2008	2009	2010	2011	2012	2013
hospodářské činy	15 921	13 906	13 382	13 365	13 247	15 857
krádeže prosté	23 230	22 657	20 947	22 130	23 678	24 500
krádeže vloupáním	9 889	10 754	11 765	12 092	11 122	13 407
majetkové TČ	37 792	38 285	37 665	39 348	40 299	43 765
mravnostní TČ	1 202	1 239	1 354	1 465	1 473	1 493
násilné TČ	11 239	10 951	12 170	13 148	12 672	12 908
ostatní kriminální činy celkem	12 835	13 908	20 440	22 334	21 569	24 336
vraždy celkem	174	157	156	148	175	165
zbývající kriminalita	48 889	49 296	32 657	32 560	30 899	30 820



5.8.3 Vývoj objasňenosti trestných činů dle typu

Tabulka 14: Procentuální objasňenost dle skupin trestných činů v letech 2008-2013

skupina TČ	2008	2009	2010	2011	2012	2013
hospodářské činy	49 %	47 %	47 %	47 %	48 %	52 %
krádeže prosté	16 %	16 %	17 %	18 %	20 %	20 %
krádeže vloupáním	19 %	20 %	20 %	20 %	20 %	21 %
majetkové TČ	17 %	18 %	18 %	19 %	21 %	21 %
mravnostní TČ	72 %	72 %	75 %	70 %	74 %	71 %
násilné TČ	63 %	65 %	67 %	68 %	69 %	69 %
ostatní kriminální činy celkem	68 %	72 %	80 %	80 %	79 %	80 %
vraždy celkem	86 %	87 %	90 %	86 %	93 %	91 %
zbývající kriminalita	91 %	93 %	91 %	90 %	90 %	89 %



5.8.4 Největší změny v objasněnosti trestných činů po nálezu ÚS

Jak naznačují grafy v předchozí kapitole, u některých skupin trestných činů mohl mít nález ÚS v březnu 2011, při kterém došlo ke zrušení data retention, a novela ZoEK s účinností od listopadu 2012 dopad na objasněnost kriminality.

V souhrnných statistikách se však tento jev prakticky neprojevil, v letech 2011 a 2012 dosahovala celková objasněnost 39 %, v roce 2013 pak 40 %.

Data retention ale samozřejmě není jediný faktor, který mohl objasněnost ovlivnit – ve statistikách ČTÚ ani MVČR však není jediný údaj, který by naznačoval spojitost žádostí s konkrétními činy.

Pro porovnání vývoje objasněnosti trestných činů v závislosti na používání provozních a lokalizačních údajů byla zvolena tři čtvrtletní časová období:

- leden 2011 – březen 2011 (platnost DR)
- leden 2012 – březen 2012 (neplatnost DR)

- leden 2013 – březen 2013 (platnost DR)⁸⁶

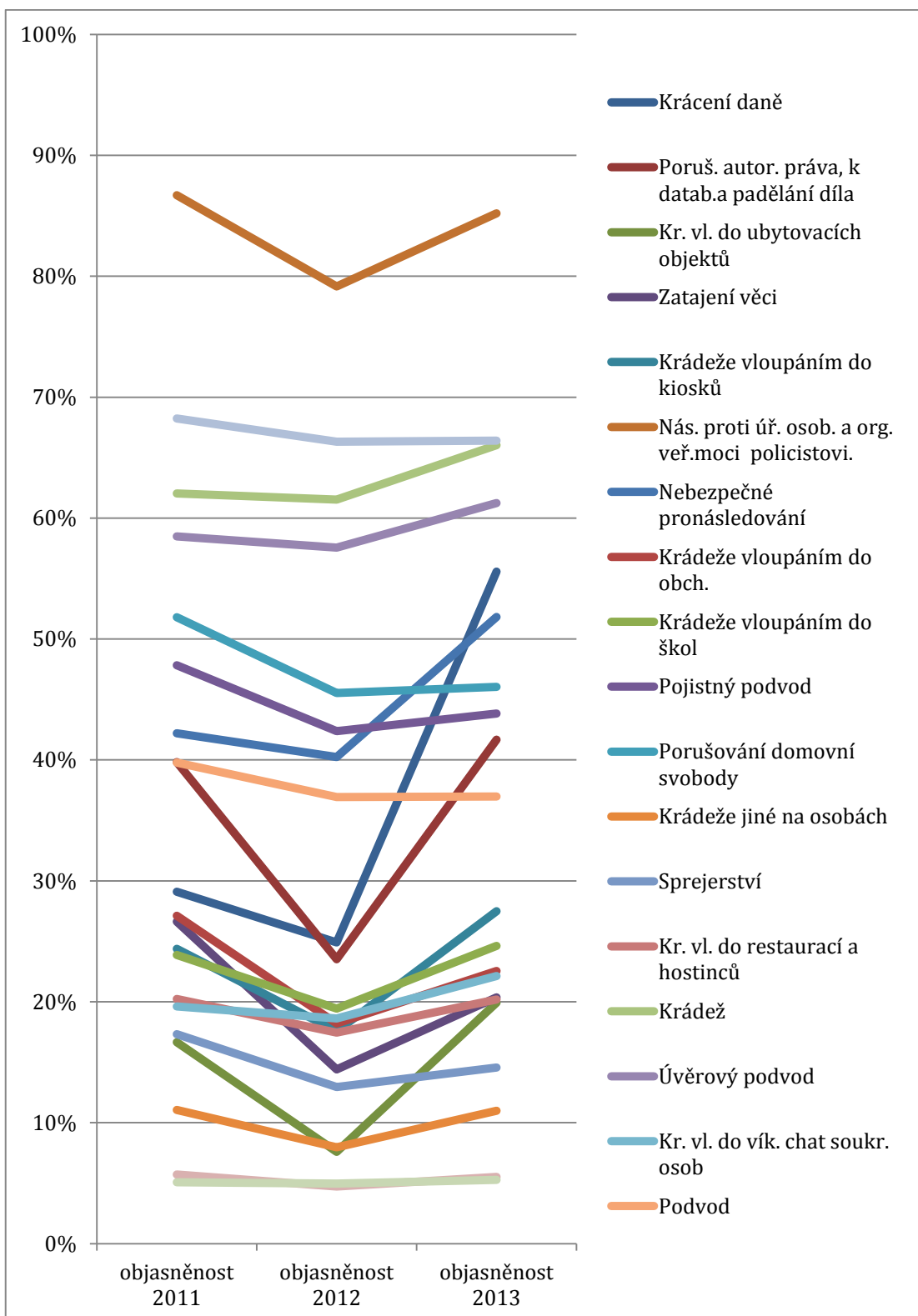
Cílem bylo najít skupiny trestných činů, u kterých došlo v procentním součtu k propadu v objasňenosti mezi stejnými období v roce 2011 a 2012 a naopak nárůstu objasňenosti mezi lety 2012 a 2013.

Tento požadavek splnilo 43 skupin činů z celkových 201. Z toho činů, které se průměrně za všechna sledovaná období stala alespoň 100x, šlo o následující skupiny (seřazeno podle nejvýraznějších změn v objasňenosti):

⁸⁶ S omezením trestných činů, pro jejichž vyšetřování je možné data retention použít.

Tabulka 15: Procentuální objasněnost vybraných trestných činů v letech 2008-2013

skupina TČ	průměrný počet spáchání	objasněnost 2011	objasněnost 2012	objasněnost 2013
Krácení daně	350	29 %	25 %	56 %
Poruš. autor. práva, k datab.a padělení díla	126	40 %	24 %	42 %
Kr. vl. do ubytovacích objektů	187	17 %	8 %	20 %
Zatajení věci	339	27 %	14 %	20 %
Krádeže vloupáním do kiosků	200	24 %	18 %	27 %
Nás. proti úř. osob. a org. veř.moci policistovi.	161	87 %	79 %	85 %
Nebezpečné pronásledování	176	42 %	40 %	52 %
Krádeže vloupáním do obch.	929	27 %	18 %	23 %
Krádeže vloupáním do škol	172	24 %	19 %	25 %
Pojistný podvod	113	48 %	42 %	44 %
Porušování domovní svobody	772	52 %	46 %	46 %
Krádeže jiné na osobách	2 073	11 %	8 %	11 %
Sprejerství	768	17 %	13 %	15 %
Kr. vl. do restaurací a hostinců	591	20 %	17 %	20 %
Krádež	133	62 %	62 %	66 %
Úvěrový podvod	1 106	58 %	58 %	61 %
Kr. vl. do vík. chat soukr. osob	1 453	20 %	19 %	22 %
Podvod	1 448	40 %	37 %	37 %
Nebezpečné vyhrožování	657	68 %	66 %	66 %
Krádeže věcí z automobilů	7 981	6 %	5 %	6 %
Ochrana měny	661	5 %	5 %	5 %



Dle názoru autora této práce data retention projevuje na objasněnosti spíše výjimečně a nepříliš výrazně (na to, že v roce 2013 bylo na 325 366 zjištěných trestných činů podáno 54 560 žádostí) a pokud, tak převážně v majetkové činnosti.

Souvislost je pravděpodobně u nebezpečného pronásledování (stalking), kde k propadu/nárůstu objasněnosti došlo a jde o čin, pro který mohou být data z DR významným důkazem.

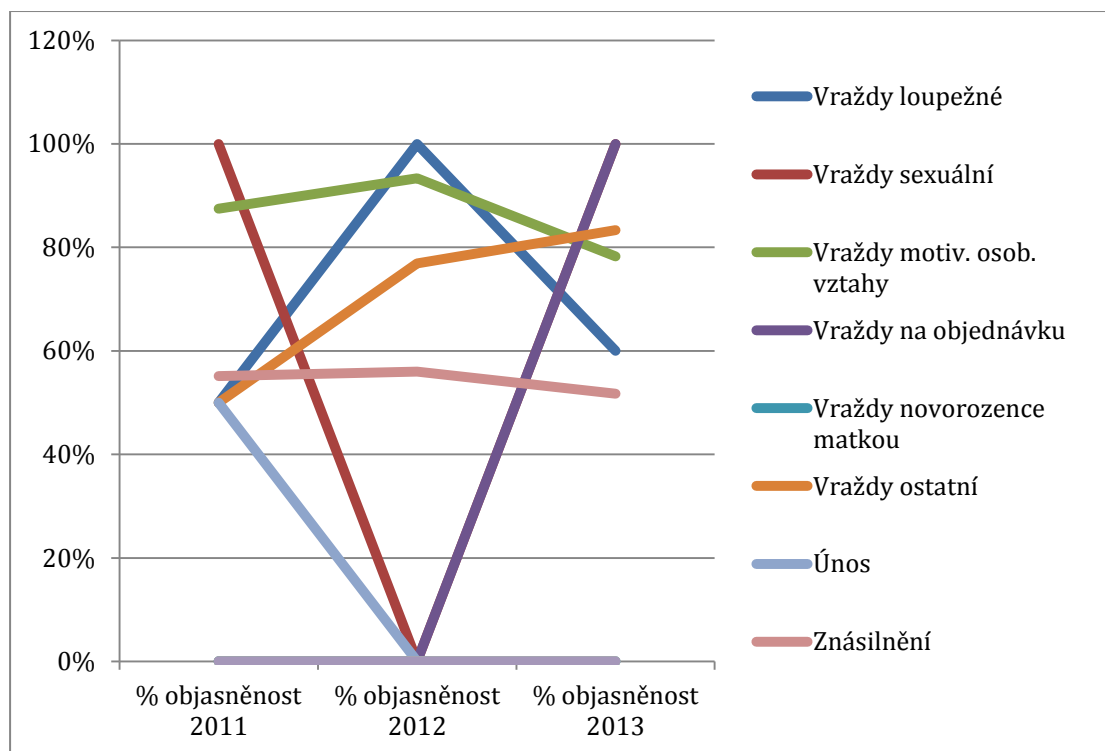
U společensky nejnebezpečnějších činů – vražd – by z těchto dat nebylo vhodné dělat závěry o DR, protože jde o statisticky malé počty, jejich objasněnost je ale tradičně poměrně vysoká a minimálně ve sledovaném období není vidět žádný dopad DR.

Oproti vraždám častější trestný čin – znásilnění – žádné změny v objasněnosti také neprojevuje.

K TČ válečným či proti ústavnímu zřízení ve sledovaném období prakticky nedošlo.

Tabulka 16: Počty zjištění, objasnění a procentuální objasněnost vybraných trestných činů v letech 2008-2013

skupiny TČ	zjišt. 2011	obj. 2011	% obj. 2011	zjišt. 2012	obj. 2012	% obj. 2012	zjišt. 2013	obj. 2013	% obj. 2013
Vraždy loupežné	2	1	50 %	6	6	100 %	5	3	60 %
Vraždy sexuální	2	2	100 %	0	0	0 %	2	2	100 %
Vraždy motiv. osob. vztahy	24	21	88 %	30	28	93 %	23	18	78 %
Vraždy na objednávku	1	0	0 %	0	0	0 %	2	2	100 %
Vraždy novorozence matkou	1	0	0 %	1	0	0 %	1	0	0 %
Vraždy ostatní	8	4	50 %	13	10	77 %	18	15	83 %
Únos	2	1	50 %	1	0	0 %	1	0	0 %
Znásilnění	156	86	55 %	216	121	56 %	147	76	52 %
Trestné činy proti ústav. zřízení	0	0	0 %	1	0	0 %	1	0	0 %
Trestné činy válečné a proti míru	0	0	0 %	0	0	0 %	0	0	0 %



5.9 Shrnutí pro rok 2013

Jak vyplývá z předchozích kapitol, na 325 tisíc zjištěných trestných činů v roce 2013 připadá 54 tisíc úkonů vyžádání dat. Pokud se dopustíme výrazného zjednodušení v podobě „jeden úkon na jeden trestný čin“, znamená to, že by se provozní a lokalizační data použila ve vyšetřování jednoho trestného činu ze šesti. V praxi bude více úkonů spojených s vyšetřováním jednoho trestného činu. Jde však o přesnější náhled pro představu o četnosti používání dat než srovnání 325 tisíc trestných činů s 198 tisíci žádostmi napočítaných operátory a nahlášených ČTÚ.

6 Závěr

Během psaní této práce prošla právní úprava data retention značnými změnami. Jednoznačně byla vyřešena otázka poskytování údajů jednotlivcům, kdy z prvotního odmítavého postupu došlo k zavedení přesných pravidel, kdy a za jakých okolností mohou uživatelé informace, které jsou o nich shromážděny, získat.

Zároveň však vznikly podněty nové, které jsou pro další pokračování sběru dat zcela zásadní a vyvolaly řadu otázek – největší je bezesporu další osud úpravy na úrovni EU. Je otázkou, zda nově vzniklá Komise připraví novou regulaci a pokud ano, zda bude mít opět formu směrnice nebo použije nařízení (tedy přímo závazný pramen bez nutnosti vnitrostátních transpozic). Tato případná nová úprava také bude mít zásadní dopad na členské státy a jejich zákony – bez této úpravy je počet států pokračujících v data retention na téměř stejný jako počet zrušení, případně nezavedení.

Samotná otázka přípustnosti těchto zásahů do soukromí zůstává stále nevyjasněná, a to jak na úrovni ČR, tak EU – vždy se najde mnoho odpůrců, kteří budou ukládání provozních a lokalizačních dat považovat za plošné sledování ne nepodobné románu 1984 od George Orwella, na druhou stranu jsou však pochopitelné potřeby policie v boji s trestnou činností, jejíž pachatelé mají díky rozvoji nových technologií cennou výhodu.

Samostatnou otázkou, která nebyla v této práci příliš zmiňována, protože se týká spíše problematiky regulace telekomunikací, je regulace OTT (Over-the-top) služeb, kam patří například Skype, WhatsApp či Facebook Messenger. Bude-li k takovéto regulaci docházet, měla by vyřešit i otázky data retention a odposlechů – aktuálně se na tyto služby zmiňované povinnosti nevztahují a představují tak pro uživatele (a případné pachatele) jistou možnost, jak alespoň některé informace skrýt.

Do budoucna by dalším rozšířením této práce mohla být analýza případné nové úpravy týkající se tohoto tématu a také obecnější otázka řešení situace v EU (nebo příslušnými orgány EU) po zrušení harmonizační směrnice, kdy došlo k rozdrobení národních úprav. Vzhledem k závažnosti tématu a nadále pokračující celospolečenské diskuzi je nepravděpodobné, že by stávající *status quo* byl dlouhodobě udržitelný.

7 Seznam použitých zdrojů

7.1 Seznam použitých právních zdrojů

BÁRTÍK, VÁCLAV, JANEČKOVÁ, EVA *Ochrana osobních údajů v aplikační praxi – vybrané otázky* 2. vyd. Praha: Linde, 2009, 262 s. ISBN 978-80-7201-813-0

DVOŘÁK, JAN a kolektiv *Občanské právo hmotné I* 1. vyd. Praha: Wolters Kluwer, 432 s. ISBN 978-80-7478-325-8

HENDRYCH, DUŠAN *Správní právo : obecná část* 7. vyd. Praha: C. H. Beck, 2009, 837 s. ISBN 978-80-7400-049-2

JELÍNEK, JIŘÍ a kolektiv *Trestní právo procesní* 3. vyd. Praha: Leges, 2013, 864 s. ISBN 978-80-87576-44-1

LLOYD, IAN, MELLOR, DAVID P. *Telecommunications law* 1. vyd. Croydon (UK): Sweet & Maxwell, 2013, 261 s. ISBN 978-0-41402-697-1

MATEJKA, JÁN *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí* 1. vyd. Praha: CZ.NIC, 2013, 256 s. ISBN 978-80-904248-7-6

MATES, PAVEL *Ochrana osobních údajů* 1. vyd. Praha: Karolinum, 73 s. ISBN 80-246-0469-8

MORAVCOVÁ, ALŽBĚTA *Právo na respektování soukromého a rodinného života ve světle judikatury Evropského soudu pro lidská práva* diplomová práce, Západočeská univerzita v Plzni, Právnická fakulta, 2012

ŠIMÍČEK, VOJTĚCH *Právo na soukromí* 1. vyd. Brno: Masarykova univerzita, 2011, 212 s. ISBN 978-80-210-5449-3

Ústavní zákon č. 2/1993 Sb., Listina základní práv a svobod

Listina základních práv Evropské unie, 2010/C 83/02

Úmluva o ochraně lidských práv a svobod

Vyhláška Federálního ministerstva zahraničních věcí č. 120/1976, Mezinárodní pakt o občanských a politických právech

Směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

Směrnice 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Zákon č. 56/1947 Sb., Telefonní řád

Zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního,

Zákon č. 40/1964 Sb. ve znění zákona č. 509/1991 Sb., občanský zákoník

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 121/2000 Sb., o ochraně osobních údajů

Zákon č. 40/2009 Sb., Trestní zákoník

Zákon č. 141/1961 Sb., Trestní řád

Zákon č. 265/2001 Sb. (novela trestního řádu)

Zákon č. 151/2000 Sb., o telekomunikacích

Zákon č. 127/2005 Sb., o elektronických komunikacích,

Zákon č. 247/2008 Sb. (novela ZoEK)

Zákon č. 153/2010 Sb. (novela ZoEK)

Zákon č. 273/2012 Sb. (novela ZoEK)

Zákon č. 182/1993 Sb., o Ústavním soudu

Zákon č. 273/2008 Sb., o policii

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

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, 485/2005 Sb.

Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, 357/2012 Sb.

Vyhláška, kterou se stanoví forma evidence provozních a lokalizačních údajů a způsob jejího předávání Českému telekomunikačnímu úřadu, 318/2010 Sb.

Vyhláška o rozsahu, formě a způsobu předávání osobních a identifikačních údajů, formě databáze těchto údajů a rozsahu, formě a způsobu předávání těchto údajů subjektu, který provozuje pracoviště pro příjem volání na čísla tísňového volání (vyhláška o předávání údajů pro účely tísňových volání), 238/2007 Sb.

Sněmovní tisk 768/1 – usnesení VOB k tisku 768/0

Sněmovní tisk 768/5

Sněmovní tisk 615/2

Sněmovní tisk 615/3

Stanovisko ÚOOÚ, UOOÚ-00159/13-2

Stanovisko pracovní skupiny 29 z 25. dubna 2006 (Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC)

Záznam z jednání Parlamentu, 5. června 2012

Data Retention and Investigatory Powers Act 2014 (Zákon Velké Británie)

Telekommunikationsgesetz , (BGBl. I S. 1190)– německý telekomunikační zákon

7.2 Seznam použité judikatury

Ústavní soud, sp. zn. I. ÚS 3038/07 z 16. října 2007, N 46/48 SbNU 549, Použitelnost odposlechu získaného dle zpravodajských zákonů v trestním řízení

Ústavní soud, sp. zn. II. ÚS 502/2000 z 22. ledna 2001, N 11/21 SbNU 83, Právo na ochranu zpráv podávaných telefonem

Ústavní soud, sp. zn. IV. ÚS 536/2000 z 13. února 2001, N 29/21 SbNU 251, Ochrana zpráv podávaných telefonem

Ústavní soud, sp. zn. IV. ÚS 78/01 z 27. srpna 2001, N 123/23 SbNU 197, K právu na ochranu zpráv podávaných telefonem - k otázce presumpce nevinny

Ústavní soud, sp. zn. Pl. ÚS 24/10 z 22. března 2011, N 52/60 SbNU 625, Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu

Ústavní soud, sp. zn. Pl. ÚS 42/11 z 20. prosince 2011

Nejvyšší soud, 21 Cdo 2058/2012 z 29. října 2013

Ústavní soud NSR, BVerfGE 65, 1 – Volkszählung, 18. října 1983

Spolkový ústavní soud (SRN)k, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08

Ústavní soud Slovenska, PL. ÚS 10/2014 z 23. dubna 2014

Ústavní soud Rumunska, rozhodnutí 1258 z 8. října 2009

Evropský soud pro lidská práva, CASE OF MALONE v. THE UNITED KINGDOM, 8691/79 z 2. srpna 1984

Rozsudek Soudního dvora (velkého senátu) ze dne 10. února 2009. Irsko proti Evropskému parlamentu a Rada Evropské unie.

Rozsudek Soudního dvora (velkého senátu) ze dne 8. října 2014, C-293/12 a C-594/12

Evropská komise vs. SRN, C-329/12 z 11. července 2012

Stanovisko generálního advokáta, C-293/12 z 12. prosince 2013

7.3 Seznam dalších zdrojů

PETERKA, JIRÍ Přednášky z MFF UK k předmětu Počítačové sítě [online]. [cit. 2013-03-19]. Dostupné z <http://www.earchiv.cz/1212/index.php3>

PETERKA, JIRÍ přednáška Historie a současný stav české mobilní telefonie [online]. [cit. 2014-11-19]. Dostupné z <http://www.earchiv.cz/papers/p70/slide.php3?l=1&me=1>

ČTÚ, tisková zpráva, Operátoři předali ČTÚ výkaz o poskytnutých provozních a lokalizačních údajích, 19. března 2014 [online]. [cit. 2014-06-01]. Dostupné z: <http://www.ctu.cz/aktuality/tiskove-zpravy.html?action=detail&ArticleId=11341>

ČTÚ, Počet případů provozních a lokalizačních údajů [online]. [cit. 2014-06-01]. Dostupné z http://www.ctu.cz/cs/download/ostatni/2014/informace_na_zadost-oldrich_kuzilek-06_03_2014-cj_9209_2014-604_e-mail.pdf

Policejní prezidium České republiky, Úřad služby kriminální policie a vyšetřování, Analýza odposlechnů a záznamu telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2013 z 6. června 2014, PPR-102-31/ČJ-2014-990390

GSMweb.cz, přehled BTS v centru Prahy [online]. [cit. 2014-10-02] Dostupné z <http://gsmweb.cz/mapa/index.php?go=1&op=all&filter=okres&okres1=AB>

GSMweb.cz, neoficiální seznamy BTS operátorů [online]. [cit. 2014-10-02] Dostupné z <http://gsmweb.cz/seznamy/index.php>

KOCMAN, ROSTISLAV Síť Telecomu je již plně digitální. *Mobil iDnes* [online]. 2002-06-28 [cit. 2014-10-28]. Dostupné z http://mobil.idnes.cz/sit-telecomu-je-jiz-plne-digitalni-d5p-/mob_tech.aspx?c=A020627_5072362_mob_ceny

PULTZNER, MARTIN Big Data ze sítě T-Mobile pomáhají na Šumavě. *Mobilenet.cz* [online]. 2014-07-30 [cit. 2014-09-02] Dostupné z <http://mobilenet.cz/clanky/big-data-ze-site-t-mobile-pomahaji-na-sumave-16710>

ŠVEC, PAVEL Pražané utíkají z města, Brňané se drží doma, ukázala data operátorů *Zprávy iDnes* [online] 2014-05-17 [cit. 2014-09-02] Dostupné z http://zpravy.idnes.cz/prazane-utekli-z-mesta-brnane-se-drzi-doma-fg7-/domaci.aspx?c=A140515_162940_domaci_itu

Zásady ochrany soukromí společnosti Google, dostupné online <http://www.google.com/intl/cs/policies/privacy/> [cit. 2014-12-02]

Vláda ČR, Mezinárodní pakt o občanských a politických právech (informační stránka) [online] 2011-09-02 [cit. 2014-10-05] Dostupné z

<http://www.vlada.cz/cz/ppov/rlp/dokumenty/zpravy-plneni-mezin-umluv/mezinarodni-pakt-o-obcanskych-a-politicky-pravech-19851/>

EISi, Slovak Constitutional Court Suspends Data Retention Legislation [online], 2014-04-24 [cit. 2014-10-05] Dostupné z <http://www.eisionline.org/index.php/projekty-m/ochrana-sukromia/74-us-data-retention-suspension>

Ústavní soud Rakouska, Gesetze zur Vorratsdatenspeicherung in Österreich verfassungswidrig (tisková zpráva) [online], 2014-07-28 [cit. 2014-10-05] Dostupné z http://web.archive.org/web/20140728100025/http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf

VASILACHE, ADRIAN Traian Basescu a promulgat asa numita 'lege Big Brother' care prevede stocarea pentru sase luni a datelor de trafic ale tuturor utilizatorilor de telefonie si internet *Hotnews.ro* [online], 2012-06-12 [cit. 2014-07-21], Dostupné z <http://economie.hotnews.ro/stiri-telecom-12503594-traian-basescu-promulgat-asa-numita-39-lege-big-brother-39-care-prevede-stocarea-pentru-sase-luni-datelor-trafic-ale-tuturor-utilizatorilor-telefonie-internet.htm> (použito pomocí překladače Google Translate)

Ústavní soud Rumunska, Tisková zpráva z 8. července 2014 [online], 2014-08-07 [cit. 2014-09-02], Dostupné z <http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99> (použito pomocí Google Translate)

JARVINEN, HEINI Data retention is here to stay despite the CJEU ruling *EDRi, Denmark* [online], 2014-06-04 [cit. 2014-07-21] Dostupné z: <https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/>

Parliament passes emergency Data Retention Bill, *BBC* [online], 2014-07-17 [cit. 2014-07-21] Dostupné z <http://www.bbc.com/news/uk-politics-28352673>

REICHL, JIŘÍ Policie umí hledat ztracené děti. Ale nesmí *Policista.cz, Lidové noviny* [online] 2008-07-01 [cit.2013-07-23] Dostupné z:

<http://www.policista.cz/clanky/reportaz/lidove-noviny-policie-umi-hledat-ztracene-deti-ale-nesmi-272/>

VOBOŘIL, JAN Data retention (nejen) v policejní praxi *Iuridicum Remedium* [online] 2012-09-25 [cit. 2014-03-04] Dostupné z

<http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf>

ŠTASTNÝ, JIŘÍ Špehování mobilů bezhlavě schvaloval jen soud v Děčíně, ukázala kontrola *Zprávy iDnes* [online] 2011-07-28 [cit. 2014-03-04] Dostupné z

http://zpravy.idnes.cz/spehovani-mobilu-bezhlave-schvaloval-jen-soud-v-decine-ukazala-kontrola-1oa-/domaci.aspx?c=A110728_134954_domaci_js

ZELENÝ, PETR Soudce nedostal trest za povolení sledování mobilů vlivných *Zprávy iDnes* [online] 2012-03-15 [cit. 2014-03-04] Dostupné z

http://zpravy.idnes.cz/nejvyssi-spravni-soud-nepotrestal-soudce-ktery-povolil-vypisy-hovoru-1nh-/krimi.aspx?c=A120315_165223_krimi_zep

KLANG, MIKULÁŠ Expolicistovi hrozí pět let za špehování mobilů soudců a Klausových lidí *Zprávy iDnes* [online] 2012-11-01 [cit. 2014-03-04] Dostupné z

http://zpravy.idnes.cz/sledovani-telefonu-weigla-nebo-rychetskeho-fe4-/krimi.aspx?c=A121101_162059_krimi_klm

PÁLKA, MATĚJ Měla honit mafiány, místo toho prý špehovala konkurenty ABL *Parlamentní listy* [online] 2012-03-12 [cit. 2014-03-04] Dostupné z

<http://www.parlamentnilisty.cz/arena/monitor/Mela-honit-mafiany-misto-toho-pry-spehovala-konkurenty-ABL-225617>

SPITZ, MALTE Your phone company is watching *TED.com* [online video] 2012-06 [cit. 2013-05-12], Dostupné z

http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

CIBULKA, JAN Co o nás ví telefon? Tři dny lidského života v datech mobilního operátora *Ihned.cz* [online] 2013-02-05 [cit. 2013-03-04] Dostupné z: http://blog.ihned.cz/c3-59259950-06b000_d-59259950-06b000_d-59259950-data-retention-zivot-v-zaznamech-mobilniho-operatora

Ceník společnosti T-Mobile [online] platný k 15. listopadu 2014 [cit. 2014-11-25] Dostupné z: https://www.t-mobile.cz/dcpublic/Cenik_sluzeb_T-Mobile.pdf

O2, Osobní údaje [online] [cit. 2014-11-25] Dostupné z: <http://www.o2.cz/osobni/202009-soukromi/313565-privacy.html>

Vodafone, Přehled tarifů a služeb [online] platný k 8. listopadu 2014 [cit. 2014-11-25] Dostupné z: http://www.vodafone.cz/_sys_/FileStorage/download/1/174/cenik.pdf

PETERKA, JIŘÍ Chcete své provozní a lokalizační údaje? Připravte si nejméně 1600 Kč *Lupa.cz* [online] 2014-08-11 [cit. 2014-11-25] Dostupné z <http://www.lupa.cz/clanky/chcete-sve-provozni-a-lokalizacni-udaje-pripravte-si-nejmene-1600-kc/>

POKORNÝ, JAKUB Co o nás ví stát? V roce 2011 jste přecházel koleje, napsala policie *Zprávy iDnes* [online] 2014-04-23 [cit. 2014-11-25] Dostupné z http://zpravy.idnes.cz/reporter-idnes-cz-zadal-urady-aby-mu-vydaly-jeho-osobni-udaje-p57-/domaci.aspx?c=A140423_123343_domaci_jp

Vodafone, vyjádření na oficiálním Twitter kanálu společnosti [online] 2013-12-03 [cit. 2014-11-25] Dostupné z https://twitter.com/Vodafone_CZ/status/407929564338610176

Ministerstvo vnitra ČR, Statistiky kriminality [online] [cit. 2014-03-29] Dostupné z: <http://www.mvcr.cz/clanek/statistiky-kriminality.aspx>

8 Seznam zkratek

(A)DSL	(Asyetric) Digital Subscriber Line
BIS	Bezpečnostní informační služba
BTS	Base Transceiver Station
CATV	Cable TV
CDR	Call Detail Record
CSD	Circuit Switched Data
ČNB	Česká národní banka
ČTÚ	Český telekomunikační úřad
DR	Data retention
EISI	European Information Society Institute
EU	Evropská unie
EÚLP	Evropská úmluva o lidských právech
GPS	Global Positioning System
GSM	Global System for Mobile (Communication)
HSCSD	High Speed Circuit Switched Data
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LZPS	Listina základních práv a svobod
MSISDN	Mobile Station International Subscriber Directory Number
MV ČR	Ministerstvo vnitra ČR
OČTŘ	Orgány činné v trestním řízení
OTT	Over the top
PČR	Policie ČR
POP3	Post Office Protocol
PSP	Poslanecká sněmovna Parlamentu
Sb.	Sbírky
SD EU	Soudní dvůr Evropské unie
SEU	Smlouva o EU
SFEU	Smlouva o fungování EU
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SRN	Spolková Republika Německo
TČ	Trestný čin
TrŘ	Trestní řád
ÚOOÚ	Úřad pro ochranu osobních údajů
URL	Uniform Resource Locator
ÚS	Ústavní soud
VOB	Výbor pro obranu a bezpečnost
VoIP	Voice over IP
ZoEK	Zákon o elektronických komunikacích

9 Anotace

Tato diplomová práce popisuje problematiku ukládání provozních a lokalizačních dat (data retention) u poskytovatelů telekomunikačních služeb. Popisuje vývoj zákonné úpravy v ČR a EU, rozhodující nálezy ústavních soudů a ESD a otázku souladu či rozporu data retention s právem na soukromí jednotlivců. Také se věnuje souvisejícím otázkám jako poskytování těchto údajů konkrétním uživatelům. V práci je také popsán technický rozsah ukládaných dat a jejich základní význam a porovnání vývoje trestné činnosti v závislosti na platnosti či neplatnosti úpravy.

10 Abstract

Data retention – storing of traffic and location metadata

The topic of this thesis is data retention – traffic and location metadata storing (and providing to state) by telecommunication providers according to Czech and European law (including rulings of constitutional courts). It also describes compliance or conflict with the users right to privacy and also possibilities to provide this data to users. There is also technical description of the data with their meaning and statistics of crimes detection according to validity of this law.

11 Seznam obrázků

Obrázek 1: Příklad mapy BTS jednoho z operátorů v centru Prahy

12 Seznam tabulek

Tabulka 1: Provozní data ukládaná v pevné telefonní síti dle vyhlášky č. 357/2012 Sb.

Tabulka 2: Provozní a lokalizační data ukládaná v mobilní síti dle vyhlášky č. 357/2012 Sb.

Tabulka 3: Provozní data ukládaná v sítích s přepojováním paketů dle vyhlášky č. 357/2012 Sb.

Tabulka 4: Provozní data ukládaná v mobilních sítích s přepojováním paketů dle vyhlášky č. 357/2012 Sb. (doplnění tabulky 3)

Tabulka 5: Provozní data ukládaná u přístupu ke schránce dle vyhlášky č. 357/2012 Sb.

Tabulka 6: Provozní data ukládaná při odesílání elektronické pošty dle vyhlášky č. 357/2012 Sb.

Tabulka 7: Provozní data ukládaná u IP telefonie dle vyhlášky č. 357/2012 Sb.

Tabulka 8: Počty poskytnutých a neposkytnutých provozních údajů v letech 2008-2013

Tabulka 9: Druhy komunikace v poskytnutých provozních datech v letech 2008-2013

Tabulka 10: Stáří poskytnutých provozních údajů v letech 2008-2013

Tabulka 11: Počty zjištěných a objasněných trestných činů 2008-2013

Tabulka 12: Skupiny trestných činů zjištěných v letech 2008-2013

Tabulka 13: Skupiny trestných činů objasněných v letech 2008-2013

Tabulka 14: Procentuální objasněnost dle skupin trestných činů v letech 2008-2013

Tabulka 15: Procentuální objasněnost vybraných trestných činů v letech 2008-2013

Tabulka 16: Počty zjištění, objasnění a procentuální objasněnost vybraných trestných činů v letech 2008-2013

13 Seznam příloh

Vyjádření společnosti O2 k poskytování provozních dat pro účely vyúčtování, JUDr.
Michal Krejčík, 10. 10. 2014

14 Přílohy

14.1 Vyjádření O2 k poskytování provozních dat pro účely vyúčtování

Pokud je odpůrce v žádosti ČTÚ vyzván ke sdělení, za jaké služby navrhovatel vyčerpал balíček Internet Evropa M, pak k tomuto požadavku odpůrce sděluje, že tzv. URL adresa umožňující přesnou specifikaci umístění zdrojů informací není provozní údaj, který by sloužil ke zpoplatnění služeb a ani není údajem, ze kterého by bylo možné dovést cenu služby ve smyslu § 90 zákona o elektronických komunikacích. Odpůrce tedy, stejně jako jiní podnikatelé v oblasti elektronických komunikací, zpoplatňuje připojení (tj. přenesené údaje) nikoli jejich obsah.

Proto také podle § 61 odst. 5) zákona o elektronických komunikacích platí, že podnikatel poskytující veřejně dostupnou službu elektronických komunikací neodpovídá při poskytování této služby za obsah přenášených zpráv. Takový podnikatel dále ani není oprávněn sledovat obsah poskytovaných služeb nebo přenášených zpráv. Naopak je povinen zajistit jejich důvěrnost a obsah neukládat. Podobnou logikou by poté bylo možné požadovat obsah zaslaných SMS zpráv a ne údaje o tom, že SMS zpráva byla zaslána.

Z tohoto důvodu je vždy možné doložit pouze přesné provozní údaje o jednotlivých spojeních s uvedením začátku, doby trvání, ukončení, IP adres a počet stažených dat v kB, ale nelze poskytnout údaje o obsahu služeb, tzn. informace o tom, jaké služby navrhovatel za objednaný balíček Internet Evropa M vyčerpал. Pouze těmito údaji lze doložit skutečné čerpání služeb (tedy zda a v jakém objemu byly čerpány), naopak z URL adres se toto čerpání poznat vůbec nedá (zjistí se maximálně na jaké stránky se uživatel díval, ale o „datové náročnosti“ tohoto prohlížení se nezjistí vůbec nic); navíc u řady datových spojení se URL adresa vůbec nevyskytuje

(např. stále více rozšířenější M2M⁸⁷ spojení, stahování aplikací či aktualizací souborů do chytrých telefonů atd. atd.).

Odpůrce, stejně jako společnost Telefónica Czech Republic, a.s. v jejíž síti odpůrce poskytuje služby elektronických komunikací, má povinnost zabezpečit důvěrnost komunikací uloženou ust. § 88 a 89 zákona o elektronických komunikacích. Jak je patrné z § 97 zákona o elektronických komunikacích a z prováděcí vyhlášky č. 357/2012 Sb., provozními a lokalizačními údaji nejsou údaje o tzv. URL adresách zmiňovaných v odůvodnění rozsudku Nejvyššího osudu ČR sp. zn. 21 Cdo 2058/2012. Tento rozsudek navíc URL adresy označuje za jeden z možných důkazů a argumentace evidentně pramenila z toho, že T-Mobile nedoložil v rámci řízení před ČTÚ žádné provozní údaje a účastník požadoval doložit „alespoň“ URL adresy. Jedná se tedy o výraz ryze civilistického pohledu na věc (poskytovatel je povinen doložit provozní údaje aby prokázal oprávněnosti vyúčtování) než na nepřímou novelizaci zákona o elektronických komunikací. Dezinterpretace ve stylu „poskytovatelé musí doložit bezpodmínečně URL adresy jinak nejsou oprávněni účtovat nic“ je zjednodušující a nikam nevedoucí výklad.

⁸⁷ Machine to machine – patří sem například vodoměry, dálkově otevíraná vrata apod.

15 Klíčová slova

data retention, provozní a lokalizační údaje, telekomunikace, právo na soukromí, zákon o elektronických komunikacích

16 Keywords

data retention, traffic and location data storing, telecommunication, privacy rights, Czech Telecommunication Act