Západočeská univerzita v Plzni
Fakulta právnická

DIPLOMOVÁ PRÁCE

UCHOVÁVÁNÍ PROVOZNÍCH A LOKALIZAČNÍCH ÚDAJŮ Z ÚSTAVNĚ PRÁVNÍHO HLEDISKA

Radek Kučera

Plzeň 2015

Západočeská univerzita v Plzni
Fakulta právnická

DIPLOMOVÁ PRÁCE

UCHOVÁVÁNÍ PROVOZNÍCH A LOKALIZAČNÍCH ÚDAJŮ Z ÚSTAVNĚ PRÁVNÍHO HLEDISKA

Radek Kučera

Plzeň 2015

Studijní program:	Právo a právní věda
Obor:	Právo
Vedoucí práce:	JUDr. Tomáš Pezl
Pracoviště:	Katedra ústavního a evropského práva

Prohlášení:

„Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.“

V Plzni dne ….. března 2015

……

Radek Kučera

Poděkování:

Na tomto místě bych rád poděkoval svému vedoucímu práce, panu JUDr. Tomáši Pezlovi, za odborné vedení i cenné rady, které přispěly ke vzniku této práce. Velké díky patří rovněž Mgr. Janu Mrázovi za jazykovou korekturu, mojí rodině a Bc. Miloši Kamarýtovi za neutuchající podporu po celou dobu studia.

Seznam zkratek

BTS	Base Transceiver Station. Základnová stanice mobilní sítě
Nákladová vyhláška	Vyhláška č. 486/2005 Sb., kterou se stanoví výše a způsob úhrady efektivně vynaložených nákladů na zřízení a zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby
Nález	Nález Ústavního soudu ze dne 23. 3. 2011, sp. zn. Pl. ÚS 24/10
Novela	Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích
Operátoři	Provozovatelé veřejně dostupné služby elektronických komunikací
Skupina 29	Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí Evropského parlamentu a Rady 95/46 ES ze dne 24. října 1995
Směrnice	Směrnice EP a Rady 2006/24 ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí
Stanovisko	Stanovisko generálního advokáta ve spojených věcech C-293/12 a C-594/12
Vyhláška	Vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
ZoEK	Zákon č. 127/2005 Sb., o elektronických komunikacích
Zpráva	Hodnotící zpráva o směrnici o uchovávání údajů

Obsah

Úvod

Dne 1. ledna 2015 vydal internetový portál mobil.idnes.cz[1] souhrnnou zprávu o počtu hovorů a SMS, které byly poslední den roku 2014 uskutečněny nebo odeslány prostřednictvím všech mobilních operátorů. Toto číslo bylo stejně jako v letech minulých opět vyšší. Celkem se jednalo přibližně o 62 milionů hovorů a 43,5 milionu textových zpráv. Každý z těchto hovorů nebo každá textová zpráva zanechala na tomto světě, po určitý čas, prakticky nesmazatelnou „digitální stopu", která je při znalosti souvislostí schopna vypovědět o každém z nás řadu informací. A tak, zatímco problematice odposlechů je dnes již věnována poměrně značná pozornost a to nejen v laických, ale rovněž i v odborných kruzích, problematika uchovávání a předávání těchto tzv. „digitálních stop" je problematika poměrně nová a z hlediska ochrany lidských práv také značně podceňovaná. Odposlechy jsou již dnes, a to i díky mnoha medializovaným kauzám, považovány za poměrně zásadní zásah do ústavou zaručených práv člověka, zatímco informace o tom, kdo, kdy a komu volal, nepovažuje většina lidí za informace, které by byly, na rozdíl od obsahu komunikace, způsobilé jakýmkoliv způsobem jejich soukromí narušit.

Bohužel, jak si ukážeme v této práci, jedná se o tragický omyl, který by, pokud by nebyl společensky regulován, hrozil přerůst pravděpodobně v nejmasovější zásah do soukromí všech dob. Z „digitálních stop" této komunikace můžeme bez potíží zjistit, kdo má jaké sociální kontakty, kdo se kde pohybuje, kde bydlí, s kým pravděpodobně žije a řadu dalších citlivých informací. Velmi obsáhle na tuto skutečnost upozornil německý poslanec Spitz, který si na základě německého zákona o ochraně osobních údajů vyžádal u německého operátora T-Mobile veškeré údaje o svém telekomunikačním provozu. Tyto následně vizualizoval a vše prostřednictvím médií zveřejnil[2]. Pro tyto „digitální stopy" používáme ustálený cizojazyčný výraz data retention, což v poněkud kostrbatém českém ekvivalentu můžeme přeložit jako „zadržování dat". Přesnější definice je pak uvedena přímo ve směrnici Evropského parlamentu a Rady 2006/24/ES, nebo ve vyhlášce č. 485/2005 Sb.[3], kdy jsou data retention vnímána jako uchovávání

[1] Češi uskutečnili 62 milionů silvestrovských hovorů. Zvýšil se i objem dat. [online]. [cit. 2015-03-21]. Dostupné z: http://mobil.idnes.cz/hovory-a-sms-o-silvestru-0xz-/mobilni-operatori.aspx?c=A150101_132220_mobilni-operatori_lhr

[2] Tell-all telephone. [online]. [cit. 2015-03-21]. Dostupné z: http://www.zeit.de/datenschutz/malte-spitz-data-retention.

[3] Podle vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí[4]. Tyto údaje můžeme rozdělit do dvou množin, přičemž první z nich jsou tzv. provozní údaje, definované v § 90 zákona č. 127/2005 Sb., o elektronických komunikací (dále jen ZoEK) jako jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování. Typicky jsou to informace o volajícím a volaném čísle, délce hovoru a ceně účtované za tento hovor. Druhou množinou jsou pak údaje lokalizační, které jsou definovány v ustanovení § 91 ZoEK takto: *„Lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“*[5]

Vzhledem k tomu, že již od roku 2001 jsem zaměstnán u společnosti T-Mobile, kde mám na starosti, mimo jiné, také poskytování těchto údajů oprávněným subjektům, zúčastnil jsem se řady jednání na různých organizačních úrovních, které se této problematiky týkaly. Jsem tak přesvědčen, že jsem schopen ve své diplomové práci přinést ucelený pohled na problematiku data retention, a to nejen v historických, technických, či právních souvislostech, ale rovněž i v souvislostech praktických, které bezprostředně souvisí s naplňováním litery příslušných zákonů v praxi. To je také hlavním cílem mojí práce. Vzhledem k tomu, že ústavní soudy patří v zemích, kde existuje specializovaná a centralizovaná struktura ústavního soudnictví k zásadním „hlídačům“ lidských práv, rozhodl jsem se podrobit data retention kritickému pohledu z pohledu ústavního a evropského práva, neboť jak bude dále patrné, otázky porušování lidských práv, ke kterým dochází v souvislosti s data retention, jsou otázkami, které dnes řeší nejen Česká republika, ale celá Evropská unie.

Pro svou práci jsem zvolil komparativní metodu s cílem porovnat některá zásadní a klíčová rozhodnutí ústavních soudů národních států či Soudního dvoru Evropské unie s rozhodnutími či názory Ústavního soudu České republiky. Pochopitelnou součástí mojí práce bude rovněž analýza právních předpisů a rozhodnutí, které se vztahují k této problematice z hlediska jejich ústavní konformity.

[4] Podle Směrnice Evropského parlamentu a Rady 2006/24/ES.
[5] Podle § 91 zákona č. 127/2005 Sb.

1 Vymezení pojmů odposlech a data retention

1.1 Odposlech a záznam telekomunikačního provozu

Ve své praxi narážím prakticky každodenně na skutečnost, že řadě osob pojmy odposlech a data retention splývají. Rád bych na tomto místě oba tyto pojmy detailně vysvětlil, neboť bez pochopení zásadních rozdílů se snadno dopustíme zcela mylných úvah týkající se možného zásahu do soukromí osob.

Odposlechem a záznamem telekomunikačního provozu rozumíme uchovávání obsahu komunikace mezi volajícím a volaným subjektem, v případě konferenčních hovorů mezi více subjekty navzájem. Stejně tak v případě počítačového provozu je to odchytávání a uchovávání obsahu datových paketů mezi uživatelem a cílovou adresou (tzn. druhým uživatelem) v prostředí internetu. Zásadním rozdílem oproti data retention je fakt, že odposlechy jsou realizovány od okamžiku aktivace zájmového čísla[6], případně IP adresy v síti operátora, a to vždy a výhradně do budoucnosti.

Není tedy pravdou, že by snad operátor či orgány činné v trestním řízení zaznamenávaly obsahy veškeré komunikace v mobilních či datových sítích. Kromě zjevné nezákonnosti takového postupu je to rovněž technicky prakticky nemožné. Jak si řekneme dále, předchází příkazu k odposlechu konkrétního čísla poměrně složitá procedura[7], která částečně omezuje svévoli jakéhokoliv orgánu veřejné moci, který by mohl mít na získání obsahu komunikace zájem. Zásadním omezením je ale jednoduše fakt, že poté, co je hovor ukončen, nikde v síti operátora, či kohokoliv jiného neexistuje záznam tohoto hovoru.

Rovněž je třeba vyvrátit další z obecně přijímaných mýtů, že operátor sám své zákazníky „odposlouchává“. I v případě soudně nařízeného odposlechu jdou veškerá data přímo k oprávněnému orgánu, který si odposlech vyžádal, resp. jej nařídil. Obecně přijímanou hypotézou je tedy skutečnost, že odposlech je podstatně větším zásahem do soukromí, nežli data retention. To může platit, ale pouze v případě, že je již tento odposlech nařízen a obsah komunikace je předán orgánu, který odposlech nařídil. V obecné rovině je, dle mého názoru, podstatně větším zásahem do soukromí právě data retention. Argumenty předkládám v následujících kapitolách.

[6] Zájmové číslo je ustálený výraz pro telefonní číslo, které je předmětem odposlechu.
[7] Podle § 88 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

1.2 Data retention

Zatímco u odposlechu dochází k zachytávání obsahu komunikace od okamžiku aktivace odposlechu směrem do budoucnosti, u data retention je tomu přesně naopak. Tato data jsou uchovávána vždy směrem do minulosti, a to v České republice až po dobu 6 měsíců zpětně[8]. Tato data jsou vytvářena v síti operátorů nepřetržitě a kontinuálně a, na rozdíl od obsahu samotné komunikace, nikam nemizí, ale operátor je uchovává. Částečně je to z důvodů potřeb samotného operátora, neboť tato data nezbytně potřebuje k vyúčtování telekomunikačních služeb či k řešení zákaznických reklamací. Avšak druhým důvodem jejich uchovávání je povinnost tato data na vyžádání oprávněných orgánů poskytnout. Co je však z hlediska ochrany soukromí naprosto klíčové je jednoduše fakt, že tato data jsou uchovávána plošně o všech účastnících sítí, bez jakékoliv výjimky. Evropský inspektor osobních údajů Peter Hustinx označil mimochodem směrnici o data retention za nejinvazivnější nástroj zásahu do soukromí, který kdy byl přijat[9]. Zdá se tedy, že podezřelým se může stát každý z nás.

1.3 Kdo má povinnost data uchovávat

Jak vyplývá z ustanovení § 97 odst. 3 zák. č. 127/2005 Sb., o elektronických komunikacích v platném znění, tak *„(…) právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací.“*[10] To v praxi znamená, že tyto údaje uchovávají primárně telefonní operátoři a poskytovatelé připojení k internetu, ať se již jedná o poskytovatele kabelového nebo ADSL připojení či jednoduše poskytovatele veřejné komunikační sítě. Určitým vodítkem je pak povinná registrace těchto subjektů u Českého telekomunikačního úřadu.[11]

[8] Podle § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích.
[9] HUSTINX, Peter. The moment of truth for the Data Retention Directive. [online]. [cit. 2015-03-22]. Dostupné z: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf
[10] Podle § 97 odst. 3 zákona č. 127/2005 Sb.
[11] Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění. [online]. [cit. 2015-03-22]. Dostupné z: http://www.ctu.cz/ctu-online/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.html

Naopak poskytovatelé služeb, jakými je většina českých internetových portálů (seznam.cz, centrum.cz apod.) takovou povinnost ze zákona nemají, neboť na tyto subjekty se vztahuje zák. č. 480/2004 Sb., o některých službách informační společnosti. Rovněž se tato povinnost nevztahuje na provozovatele sítí, které jsou neveřejné, typicky např. školní, univerzitní nebo knihovní wi-fi sítě. To se zdá být v otázce ochrany soukromí dobrou zprávou, skutečnost je ale taková, že již dnes probíhají na evropské i národní platformě diskuse o možnosti rozšíření povinnosti data retention i o subjekty poskytující internetové služby. Je to z toho důvodu, že subjektů, které poskytují internetové služby je pochopitelně mnohem více, nežli poskytovatelů veřejně dostupné služby elektronických komunikací. Stejně tak je nutné upozornit na snahu některých zákonodárců o regulaci odvětví poskytovatelů internetového obsahu, kteří by měli za povinnost dohlížet na dodržování autorských práv a ochranu duševního vlastnictví. Tyto snahy však byly prozatím občanskou společností ostře kritizovány a odmítnuty[12].

1.4 Data retention prakticky

Abychom v následujících kapitolách dokázali dobře pochopit, o co vlastně v uchovávání provozních a lokalizačních údajů jde, bude následující kapitola věnována vysvětlení některých klíčových pojmů z technického a praktického hlediska. Veškerý popis bude silně zjednodušený, určený pouze pro pochopení toho kde, jak a proč se berou provozní a lokalizační údaje.

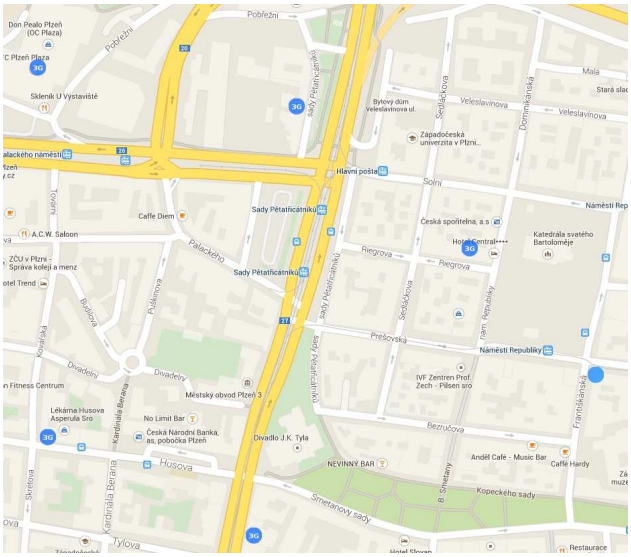
O uchovávání provozních a lokalizačních údajů má smysl hovořit až v souvislosti s digitalizací pevných a nástupem digitálních mobilních telefonních sítí. U digitálních pevných sítí je poloha i identita uživatele dobře známa, a tak již např. v devadesátých letech byla tato vlastnost běžně využívána pro lokalizování člověka volajícího z pevné linky na linku tísňového volání, kdy operátor při přijetí takového volání věděl, na jaké adresa je pevná linka umístěna, komu patří a kam má tedy vyslat složky integrovaného záchranného systému. U mobilního telefonu je šíření signálu zajišťováno pochopitelně nikoliv „kabelem“, ale prostřednictvím tzv. základnových stanic, tzv. BTS[13]. Tyto základnové stanice šíří mobilní signál, pomocí kterého může koncový uživatel uskutečnit hlasové či datové spojení. Každý

[12] ACTA skončila. Europoslanci ji definitivně zamítli drtivou většinou. [online]. [cit. 2015-03-22]. Dostupné z: http://technet.idnes.cz/acta-skoncila-europarlament-zamitl-actu-fdq-/sw_internet.aspx?c=A120704_132333_sw_internet_pka

[13] Zkratka z anglického„Base Transceiver Station“.

z operátorů má v České republice něco kolem 7 tisíc takových BTS[14]. Čím vyšší je hustota takových stanic, tím přesněji je známa poloha mobilního telefonu.

Obr. 1. Umístění BTS v Plzni. Ukázka hustoty umístění základnových stanic GSM operátora T-Mobile (modré body) v Plzni – okolí Právnické fakulty.



(Zdroj: Interaktivní mapa BTS. [online]. [cit. 2015-03-22]. Dostupné z: http://www.gsmweb.cz/mapa)

Pokud se chce uživatel A spojit s uživatelem B, musí mobilní síť vědět, kam má takový hovor směrovat. Z tohoto důvodu si musí mobilní síť pamatovat, v jaké teritoriální oblasti se nachází mobilní telefon uživatele B, resp. mobilní telefony všech účastníků mobilní sítě. To mobilní síť zjistí vždy při přihlášení telefonu do sítě a vždy, když uživatel mobilního telefonu přejíždí mezi jednotlivými BTS. I pokud je uživatel doma, ověří si síť nejméně jednou za 4 hodiny, že je telefon stále na BTS, kde byl naposledy přihlášen. Síť tedy spojí uživatele A a uživatele B. Součástí tohoto přenosu jsou právě ony zmiňované provozní a lokalizační údaje.

Pro zjednodušení si uvedeme ty nejdůležitější:

a) identifikace mobilního čísla A (A – party) tzv. MSISDN neboli číslo volajícího
b) identifikace mobilního čísla B (B – party) MSISDN číslo volaného
c) identifikace zařízení (telefon, datový modem apod.) dle výrobního čísla IMEI
d) typ služby (SMS, hlas, MMS, datové spojení, apod.)
e) začátek spojení

[14] Mapy BTS jsou dostupné na: www.gsmweb.cz.

f) konec spojení
g) doba trvání hovoru
h) počáteční buňka (kde byl hovor zahájen)
i) cílová buňka (kde byl hovor ukončen)

Tyto informace jsou provozovatelem sítě uchovávány a ukládány po celou zákonnou dobu 6 měsíců, kdy mohou být vyžádány orgány, které jsou k jejich vyžádání oprávněny. Z předestřeného výčtu je zřejmé, že tato data poskytují velmi cenné informace, které umožňují velmi přesně zmapovat v podstatě celý sociální život uživatele. V kombinaci s analýzou sociálních sítí, údaji z bankovních registrů a všech dalších veřejně přístupných registrů (ARES, obchodní rejstřík, atd.) získáme ucelený přehled o tom, jak člověk žije, s kým se stýká, jaké jsou jeho majetkové poměry, jeho koníčky a záliby a mnoho dalšího.

2 Právo na soukromí jako ústavně zaručené právo

2.1 Právo na soukromí v historickém kontextu

Na právo na soukromí lze dnes nahlížet mnoha různými způsoby, a to od ochrany osobnosti, tak jak je definována v Občanském zákoníku[15], přes právo na soukromí definované právní teorií, až po právo na soukromí, tak jak je definováno v ústavním pořádku či mezinárodních smlouvách. Z pochopitelných důvodů jsem si ve své práci zvolil právě zmiňovaný ústavně právní pohled.

Ústavní listina Československé republiky[16] žádné explicitní ustanovení, které se týká práva na soukromí, neobsahuje. Pouze § 116 obsahuje ústavně zaručené právo na ochranu listovního tajemství[17].

Obdobná situace je potom rovněž u zákona č. 150/1948 Sb., Ústava Československé republiky, která ve svém § 6 definuje ústavně zaručené právo na tajemství listovní a tajemství dopravovaných zpráv. Poprvé se nám zde objevuje, v souvislosti s technickým rozvojem, rovněž ochrana zpráv, která je podávána telegrafem, telefonem nebo jiným podobným veřejným zařízením[18].

Ústavní zákon č. 100/1960 Sb., Ústava Československé socialistické republiky potom ve svém čl. 31 definuje ochranu soukromí velmi zvláštním způsobem, kdy do jednoho ustanovení subsumuje nedotknutelnost obydlí, listovního tajemství, tajemství dopravovaných zpráv a dokonce svobodu pobytu[19]. Lidská práva byla v této ústavě zhuštěna do pouhých dvaceti článků v hlavě druhé. Je tak zřejmé, že ústavně zaručené právo na soukromí, obdobně jako řada jiných lidských práv, bylo v epoše socialistického státu právem ryze proklamativním, bez skutečné schopnosti toto právo svým občanům garantovat. Jak jinak si lze vysvětlit rovněž fakt, že Ústavní soud jako garant ústavnosti ve státě byl zrušen, a to již s přijetím ústavy 9. května 1948. Jak vyplývá z důvodové zprávy Národního shromáždění republiky Československé, důvodem bylo posílení významu

[15] Zákon č. 89/2012 Sb., Občanský zákoník.
[16] Ústavní zákon č. 121/1920 Sb., ze dne 29. února 1920, kterým se uvozuje Ústavní listina Československé republiky [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1920.html
[17] Tamtéž.
[18] Ústavní zákon č. 150/1948 Sb., Ústavní zákon ze dne 9. května 1948, Ústava Československé republiky [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1948.html
[19] Ústavní zákon č. 100/1960 Sb., ze dne 11. července 1960, Ústava Československé socialistické republiky. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1960.html

Národního shromáždění na nejvyšší orgán ve státě (cituji autory): *„Odstraňujeme všechny zvláštní orgány, které byly více méně byrokratické povahy a které fakticky stály nad Národním shromážděním. Mám na mysli především ústavní soud.“*[20] Smutnou skutečností potom zůstává, že Ústavní soud již nebyl až do změny společenského režimu nikdy obnoven, ačkoliv s jeho opětovným zřízením nová ústava[21] z roku 1968 počítala. Pro úplnost dodávám, že ani tato ústava právo na soukromí nijak nespecifikuje, naopak z jejího pojetí občanská práva vypadla úplně.

Jako určitou snahu přihlásit se alespoň k formálnímu dodržování lidských práv vnímám přihlášení se k Mezinárodnímu paktu o občanských a politických právech, který byl Československou socialistickou republikou podepsán dne 7. 10. 1968 a ratifikován 23. 12. 1975[22]. O tom, že respektování těchto práv, která se stala součástí právní řádu ČSSR[23], nebylo automatické, nelze mít žádné pochybnosti, na což mnohokrát poukázal např. Český helsinský výbor[24].

Ani po tzv. Sametové revoluci nedošlo, snad kromě vypuštění vedoucí úlohy Komunistické strany Československa, k přijetí moderní federální ústavy, která by dostatečně sledovala lidsko-právní oblast. Naopak v roce 1992, kdy již bylo zřejmé, že Československá federace směřuje ke svému rozdělení, se začaly oba státy tehdejší federace soustředit na vytvoření svých vlastních ústavních zákonů. Ještě před rozpadem federace byl však Federálním shromážděním ratifikován pravděpodobně nejdůležitější dokument, který se týkal lidsko-právní oblasti, a to Úmluva o ochraně lidských práv a svobod. Přestože Úmluva byla podepsána v Římě již 4. listopadu 1950, přistoupilo Československo k její ratifikaci až 18. března 1992, kdy byla publikována ve sbírce zákonů pod č. 209/1992 Sb.[25] V roce 1993 byl pak přijat zákon č. 1/1992 Sb., Ústava České republiky, a především zákon č. 2/1993 Sb., Listina základních práv a svobod. Ta sice není formálně označena jako ústavní zákon, nicméně je součástí ústavního pořádku

[20] Důvodová zpráva k návrhu nové ústavy ČSR. [online]. [cit. 2015-03-22]. Dostupné z: http://psp.cz/eknih/1946uns/tisky/t1227_06.htm
[21] Ústavní zákon č. 143/1968 Sb., o československé federaci.
[22] Vyhláška 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech. [online]. [cit. 2015-03-22]. Dostupné z: http://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/rlp/dokumenty/mezinarodni-pakt-o-obcanskych-a-politickych-pravech-a-mezinarodni-pakt-o-hospodarskych--socialnich-a-kulturnich-pravech-19852
[23] Tamtéž.
[24] Český helsinský výbor - historie. [online]. [cit. 2015-03-22]. Dostupné z: http://www.helcom.cz/cs/o-nas/historie/
[25] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=209&r=1992

České republiky a pramenem ústavního práva. Její právní síla je pak s ústavními zákony plně srovnatelná.

2.2 Pojetí práva na soukromí v současné době

Listina základních práv a svobod přinesla poprvé v naší novodobé historii ucelený a systematický pohled na ústavně zaručená práva člověka. Již z prvního článku Listiny základních práv a svobod je patrná inspirace jiným významným ústavním dokumentem, a sice Deklarací práv člověka a občana, která byla ve Francii vydána 26. srpna 1789 francouzským Ústavodárným národním shromážděním a představovala významný krok k současnému evropskému pojetí lidských práv. Stejně tak vychází Listina základních práv a svobod ve svém výčtu z katalogu lidských práv, vyjmenovaných ve Všeobecné deklaraci lidských práv přijaté již 10. 12. 1948 Valným shromážděním Organizace spojených národů. Rozhodně v této souvislosti stojí za připomenutí, že tehdejší Sovětský svaz ani Československo tuto deklaraci neratifikovaly, ale hlasování se zdržely[26].

Ústava a Listina nebyly jedinými dokumenty, které byly v souvislosti s lidskými právy přijaty. Česká republika rovněž přejala jak v předchozí kapitole zmiňovaný Pakt o občanských a politických svobodách[27], tak i oba opční protokoly[28], a především evropskou Úmluvu o ochraně lidských práv a svobod[29].

Listina základních lidských práv a svobod nijak uceleně právo na soukromí nespecifikuje. Naopak ochranu tohoto práva rozprostírá mezi několik článků. Konkrétně se jedná o článek 7 odst. 1 Listiny, který konstatuje, že nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem. Dále článek 10 ve všech třech odstavcích, ve kterých Listina zaručuje adresátům ochranu důstojnosti, cti, dobrého jména, ochranu soukromého a rodinného života, stejně jako ochranu před neoprávněným shromažďováním, zveřejňováním, či zneužíváním údajů o své osobě. Nedotknutelnost obydlí je pak garantována v článku 12 a oblast, která nás v souvislosti s odposlechy či

[26] Vote of the General Assembly to Adopt the Universal Declaration of Human Rights (UDHR). [online]. [cit. 2015-03-22]. Dostupné z: http://www.gcc.ca/pdf/INT000000019b.pdf
[27] Sdělení Ministerstva zahraničních věcí č. 100/2004 Sb.m.s. [online]. [cit. 2015-03-22]. Dostupné z: http://www.gcc.ca/pdf/INT000000019b.pdf
[28] Sdělení federálního ministerstva zahraničních věcí č. 169/1991 Sb. [online]. [cit. 2015-03-22]. Dostupné z: http://www.nssoud.cz/zakony/169_1991.pdf
[29] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=209&r=1992

uchováváním provozních a lokalizačních údajů zajímá nejvíce, pak v článku 13, podle kterého: *„(…)nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“*[30] Úmluva je potom ve svém výčtu ještě stručnější a podřazuje právo na soukromí komplexně pod článek 8 odst. 1: *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.“*[31] Z předestřeného výčtu je zřejmé, že při definici soukromí si tak musíme vypomoci spíše judikáty ústavních soudů či názory soudců.

2.3 Právo na soukromí pohledem soudců

Bývalá ústavní soudkyně Eliška Wagnerová definuje soukromí jako fenomén, který se rozprostírá do čtyř hlavních oblastí[32]:

1. Právo na osobní soukromou sféru
2. Právo na uzavření manželství a založení rodiny
3. Právo na soukromí v prostorové dimenzi
4. Soukromí jako důvěrnost komunikace

Právo na osobní soukromou sféru poté Wagnerová definuje jako právo, které kromě osobnostních práv zahrnuje rovněž právo každé osoby na informační sebeurčení a právo autonomně rozhodovat o osobní integritě. Pod právo na informační sebeurčení Wagnerová subsumuje ochranu člověka před hlídáním a sledováním ze strany veřejné moci, byť připouští, že v rámci ochrany bezpečnosti států či života a zdraví osob je přípustné používání některé z forem plošného sledování osob, jakými jsou např. všudypřítomné bezpečnostní kamery. Zdůrazňuje však, že taková opatření musí vždy projít ústavně právními testy. Za mimořádně přínosné pak považuji varování, že k přijetí podobných opatření nepostačuje pouze „obecné napětí“ ve společnosti, či mezinárodně politické napětí[33].

[30] Článek 13 zákona č. 2/1993 Sb., Listina základních práv a svobod.
[31] Článek 8 odstavec 1 zákona č. 2/1993 Sb., Listina základních práv a svobod.
[32] WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být i soukromí. In: *Právo na soukromí.* Editor Vojtěch Šimíček. DOI: ISBN 978-80-210-5449-3.
[33] Tamtéž, s. 54-59.

Bohužel, prakticky jakékoliv zhoršení světové bezpečnostní situace či teroristický útok spáchaný v Evropě posiluje přesvědčení některých zákonodárců, že stát by měl „preventivně“ zasahovat do soukromí občanů, a to jejich sledováním kdykoliv a kdekoliv. Za obzvláště nebezpečné pak považuji společenské mínění reprezentované názorem „pokud nic špatného nedělám, nemám se čeho bát.“

Autonomní rozhodování o osobní integritě není z pohledu této práce relevantní, neboť mezi dotčená práva v tomto případě patří právo na přerušení těhotenství či právo na sexuální sebeurčení, včetně sexuální orientace. Stejně tak není potřeba se pro účel této práce zabývat právem na uzavření manželství, rodinný život či právem v prostorové dimenzi, tedy nedotknutelnost obydlí.

Naopak právo na důvěrnost komunikace je právem, které bylo v minulosti, kvůli neexistenci pokročilých komunikačních technologií, zúženo spíše na korespondenci či zprávy předávané telegrafem, avšak v současné době můžeme do této oblasti zahrnout prakticky jakoukoliv komunikaci prostřednictvím telefonu nebo počítače. Zatímco v oblasti běžného hovoru či e-mailové komunikace není o povaze toho, co je potřeba chránit nejmenších pochybností, velkou výzvou v dnešní době zůstává ochrana soukromí na sociálních sítích, kde není zcela zřejmé, zda informace, které o sobě sděluje uživatel sociálních sítí (typicky Facebook) má povahu veřejnou, či soukromou, která si zasluhuje nějakou formu právní ochrany.

Prof. Ján Svák obsahově vymezuje právo na soukromí jako právo, které se opírá o 6 pilířů[34]:

1. Zákaz shromažďování a uchovávání osobních údajů
2. Práva spojená s menšinovou sexuální orientací
3. Právo na ochranu dobrého jména a cti
4. Ochranu obydlí a domovní svobodu
5. Ochranu korespondence a tajemství dopravovaných zpráv
6. Právo na ochranu životního prostředí

Ján Svák pak pod ochranu korespondence podřazuje právo na nerušenou a důvěrnou komunikaci s jinými lidmi, přičemž pod pojem korespondence řadí veškeré hlasové či obrazové přenosy, dále chaty, elektronickou poštu, Skype, ICQ a jiné podobné messengery, stejně jako korespondenci osobní, kterou nevnímá pouze v listinné podobě, ale rovněž k ní řadí např. záznam hlasu na diktafon.

[34] SVÁK, Ján. Ochrana ľudských práv: (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv). 2. rozš. vyd. Žilina: Poradca podnikateľa, 2006, s. 425. ISBN 8088931517.

Doc. Čentéš ve své publikaci týkající se procesně právních a hmotně právních aspektů odposlechu cituje angloamerický pohled na vnímání konceptu soukromí. Tento pohled je reprezentován soudcem Brandeisem ve věci Olmstead vs. U.S. 438, 478, 1928: „*Tvůrci naší ústavy na sebe vzali odpovědnost vytvořit příznivé podmínky pro usilování o štěstí. Přiznali právo (proti státu) být ponechán sám sebou – což je nejkomplexnější a nejobsažnější právo ze všech a zároveň právo, které je nejvzácnější civilizovanému lidstvu. A tak se z práva na soukromí stal jeden ze základních elementů Ústavy USA, které zabezpečuje autonomii jednotlivce.*“[35]

Jak dodává doc. Čenteš, je „*(…) soukromí chápané jako prostor, kde se jednotlivec svobodně vyvíjí a realizuje svou osobnost podle vlastních představ, bez zbytečných omezení, příkazů a zákazů ze strany veřejné moci. Účelem práva na soukromí je pak ochrana jednotlivce před svévolným a nepřiměřeným zásahem veřejné moci do jeho soukromí.*“[36] Mezi takový zásah pak nepochybně patří nejen odposlech, ale i uchovávání provozních a lokalizačních údajů.

2.4 Vybrané judikáty

2.4.1 Malone vs. Spojené království

V roce 1977 byl James Malone, britský obchodník se starožitnostmi, obviněn z trestných činů v souvislosti s nakládáním se zbožím. Tohoto obvinění bylo dosaženo, mimo jiné na základě využití odposlechů a monitoringu korespondence. Vláda Spojeného království byla přesvědčena, že veškeré sledování bylo legální, neboť bylo schváleno státním tajemníkem a byly splněny veškeré podmínky pro nasazení tak závažného nástroje. Malone však tvrdil, že několikaleté odposlouchávání jeho telefonů a monitorování obsahu jeho korespondence bylo nelegální, a z tohoto důvodu podal žalobu k Evropskému soudu pro lidská práva. Soud konstatoval, že vnitřní předpisy Spojeného království dostatečně nespecifikují podmínky, za kterých je možné odposlech nařídit, čímž došlo k porušení čl. 8 Úmluvy o ochraně lidských práv a svobod.[37]

[35] ČENTÉŠ, Jozef. Odpočúvanie, procesnoprávne a hmotnoprávne aspekty. Prvé vydanie. s. 1. ISBN 9788089603091.
[36] Tamtéž, s. 2.
[37] Rozhodnutí ve věci *Malone proti UK* (no. 8691/79) ze dne 2. 8. 1984.

2.4.2 Chadimová vs. Česká republika

Marta Chadimová požádala na podzim 1991 bytový podnik o vydání domu na Loretánském náměstí. Celkem šlo o majetek v hodnotě přibližně 40 milionů korun. V roce 1992 však bylo na Chadimovou podáno trestní oznámení a policie ji obvinila, že se snažila majetek získat neoprávněně a padělala kvůli tomu veřejné listiny včetně zápisů v zemských deskách a pozemkových knihách. Martě Chadimové byly v této věci odposlouchávány rovněž telefonní hovory. V roce 1995 nařídil Ústavní soud zničení těchto odposlechů, což se však v plné šíři nestalo. Evropský soud pro lidská práva pak v následné stížnosti rozhodl, že délka řízení před českými soudy byla příliš dlouhá a rovněž, že nesplněním povinnosti uložené Ústavním soudem došlo k porušení práva na soukromí, tak jak je definováno v článku 8 Úmluvy o ochraně lidských práv a svobod[38].

2.4.3 Heglas vs. Česká republika

V roce 2000 byl na devět let odsouzen Vojtěch Heglas, kterému bylo prokázáno loupežné přepadení, kdy se spolupachatelem napadl ženu a za použití násilí jí odcizil kabelku s hotovostí ve výši 275.000,- korun. Heglasovo odsouzení bylo založeno také na poskytnutí výpisů telefonních hovorů uskutečněných mezi ním a jeho spolupachatelem v době činu a na základě záznamu rozhovoru Heglase s jednou ze svědkyň, pořízeného podle pokynů policie pomocí diktafonu ukrytého na jejím těle. Po vyčerpání opravných prostředků rozhodl Ústavní soud, že sice ani nahrávka, ani poskytnutí informací z telefonního hovoru neměly být použity jako důkaz, nicméně řada dalších důkazů svědčí o tom, že vina obžalovaného byla plně prokázána. Ústavní soud tedy Heglasovu stížnost zamítl. Evropský soud pro lidská práva pak rozhodl, že právo na respektování soukromého života bylo porušeno, neboť jak využití přehledu telefonních hovorů, tak i pořízení skrytého záznamu představuje porušení článku 8 Úmluvy o ochraně lidských práv a svobod. Navíc veškeré tyto zásahy mohou být v souladu s Úmluvou pouze za předpokladu, že nechybí jejich výslovná zákonná úprava. To se však v tomto případě nestalo, neboť zákonná úprava poskytování provozních a lokalizačních údajů byla upravena v § 88a trestního řádu až později, konkrétně nabyla účinnosti až 1. ledna 2002. Stejnou

[38] Chadimová vs. Česká republika, rozsudek ESLP, ze dne 18. dubna 2006, stížnost č. 50073/99

výtku spočívající v neexistující či nedostatečné právní úpravě soud vyslovil rovněž ve způsobu použití záznamového zařízení[39].

[39] Heglas vs. Česká republika, rozsudek ESLP ze dne 26. července 2007, stížnost č. 64209/01.

3 Vývoj právní úpravy data retention v České republice

3.1 Zákon o telekomunikacích z roku 1964

Zákon č. 110/1964 Sb., o telekomunikacích o rozsahu pouhých 26 paragrafů zakotvil ve svém § 20 pojem telekomunikačního tajemství a povinnost mlčenlivosti pracovníků organizace obstarávající provoz jednotné telekomunikační sítě o obsahu přijatých a zprostředkovaných zpráv. Údaje o dopravovaných a zprostředkovaných zprávách mohly být sdělovány pouze odesílatelům a adresátům těchto zpráv, případně jejich právním nástupcům. Soudům a jiným státním orgánům pak mohly být doprovodné a zprostředkované zprávy či údaje o nich sdělit jen v případech stanovených zákonem. S ohledem na tehdejší technickou vyspělost telekomunikací chybí přesnější vymezení pojmu „zpráva“, technický prostředek, kterým k přenosu zprávy má docházet (telefon, telegraf), či bližší konkretizace tzv. „jiných státních orgánů“, kterým bylo možné tyto údaje sdělit. Zcela pak absentuje údaj o době, po kterou by měly být zprávy uchovávány[40].

3.2 Zákon o telekomunikacích z roku 2000

Zákon č. 151/2000 Sb., o telekomunikacích byl již v otázce vymezení telekomunikačního tajemství a povinností operátorů držet údaje z telekomunikačního provozu podstatně komplexnější[41]. Konkrétně v § 86 stanovil, že:

„(1) Osoby uvedené v § 84 odst. 1 jsou povinny na vlastní náklady sdělit orgánům oprávněným k tomu zvláštními právními předpisy[42] 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. U poskytovaných datových celků (databází) jsou tyto osoby povinny provádět jejich aktualizaci podle požadavků orgánů oprávněných k tomu zvláštními právními předpisy, nejméně jednou za 6 měsíců.

[40] Zákon č. 110/1964 Sb., o telekomunikacích. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=110&r=1964
[41] Podle § 84 a 86 zákona č. 151/200 Sb., o telekomunikacích.
[42] Například zákon č. 67/1992 Sb., zákon č. 154/1994 Sb., zákon č. 283/1991 Sb., zákon č. 141/1961 Sb., a zákon č. 13/1993 Sb.

(2) Právnické a fyzické osoby, které vykonávají telekomunikační činnost, jsou povinny na vlastní náklady zabezpečit v určených bodech orgánům oprávněným podle zvláštního právního předpisu připojení zařízení pro odposlouchávání a zaznamenávání telekomunikačního provozu. Technické podmínky pro připojení a provoz těchto zařízení stanoví prováděcí předpis.

(3) Pokud právnické a fyzické osoby, které vykonávají telekomunikační činnost, zavedou v telekomunikačním provozu kódování, kompresi, šifrování nebo jiný způsob utajení přenosu informací, jsou povinny zajistit, aby v místě rozhraní pro připojení zařízení uvedených v odstavci 2 byly požadované informace a data poskytovány srozumitelným způsobem.“[43]

Zmiňovaná úprava bohužel žádným způsobem nekonkretizovala poněkud vágní pojem „informace o skutečnostech, které jsou předmětem telekomunikačního tajemství“, což v praxi vytvářelo nejasnosti ohledně rozsahu uchovávaných dat, byť určitý zákonný demonstrativní výčet byl v paragrafovém znění obsažen. Stejně tak tato právní úprava nepracovala s pojmy „provozní a lokalizační údaje“ nebo dokonce „data retention“. Mezi další praktické problémy bylo možné zařadit:

a) zákon taxativně neurčil osoby, které jsou oprávněné data vyžadovat, pouze odkázal na speciální zákony. Více o způsobu vyžadování dat v kapitole 3.6.
b) Zákon stanovil, že data je provozovatel telekomunikační sítě povinen uchovávat a oprávněným orgánům poskytovat na vlastní náklady. Více o hrazení nákladů v kapitole 4.

3.3 Zákon o elektronických komunikacích z roku 2005

K urychlení diskusí o změnách legislativy týkající se povinnosti uchovávat a poskytovat provozní a lokalizační údaje významně přispěla změna politické situace po roce 2001, kdy byl proveden teroristický útok na budovy Světového obchodního centra a Pentagonu. Přijatá Směrnice Evropského parlamentu a Rady č. 2002/58/ES[44] zakotvila ve svém článku 15 oprávnění členských států zavést

[43] Podle § 86 zákona č. 151/200 Sb., o telekomunikacích.
[44] Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS

legislativní opatření umožňující držet data po určitou dobu, a to z důvodů *„(…) zajištění národní bezpečnosti, obrany, veřejné bezpečnosti, a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému.“*[45] Stejně tak ovšem tato směrnice v článku 15 upozorňuje, že *„veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o založení Evropské unie.“*[46] Je třeba zdůraznit, že se jednalo pouze o právo každého členského státu, a nikoliv povinnost. Jak ze samotného textu vyplývá, zmiňované právo je velmi široce formulováno a poskytuje zákonodárcům nebezpečně velký manévrovací prostor, což se ukázalo ve způsobu přijímání tohoto oprávnění v jednotlivých státech. Česká republika transponovala toto oprávnění velmi horlivě, a to téměř rok předtím, nežli byla přijata speciální úprava data retention představovaná směrnicí 2006/24/ES. Čeští zákonodárci zakotvili tuto povinnost v zákoně č. 127/2005 Sb., o elektronických komunikacích, který nabyl účinnosti 1. května roku 2005.

V ustanovení § 97 pak zákonodárci vymezili povinnosti provozovatelů sítí elektronických komunikací, které se týkaly jak odposlechů a záznamu telekomunikačního provozu, tak především uchovávání provozních a lokalizačních údajů. V § 97 odst. 3 je stanoveno, že: *„právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, je povinna uchovávat provozní a lokalizační údaje, a tyto údaje je na požádání povinna poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu. Rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců, a formu a způsob jejich předávání orgánům oprávněným k jejich využívání, stanoví prováděcí právní předpis.“*[47]

Kromě povinností, které se vztahovaly k povinnostem provozovatelů sítí elektronických komunikací, došlo k přijetí legislativního prvku, který významně reguloval, aby nedocházelo k nadužívání informací u bagatelních trestných činů, ačkoliv to pravděpodobně nebylo jeho původním smyslem. Tímto prvkem byla

[45] Čl. 15 směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS)

[46] Zásady svobody, demokracie, dodržování lidských práv a základních svobod. (Čl. 15 směrnice Evropského parlamentu a Rady 2002/58/ES.)

[47] Zákon č. 154/1994 Sb., o BIS, zákon č. 289/2005 Sb., o Vojenském zpravodajství, zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 141/1961 Sb., trestní řád. (§ 97 odst. 3 zákona č. 127/2005 Sb.)

úhrada nákladů za uchovávání a poskytování informací. Poprvé tak došlo k tomu, že poměrně značné náklady, které musí provozovatel sítí vynaložit v souvislosti s uchováváním a poskytováním těchto informací, získal zpět ze státního rozpočtu. Toto ustanovení zakotvené v ZoEK[48] bylo velmi pokrokové, neboť jsme byli s výjimkou Velké Británie a Finska jedinou evropskou zemí, kde k hrazení nákladů tímto způsobem a v tomto rozsahu došlo. Zasloužil se o to Hospodářský výbor Sněmovny, neboť v legislativním návrhu měly být původně veškeré náklady k tíži poskytovatele.

Již v prvních měsících po nabytí účinnosti se ukázalo, že demonstrativní výčet subjektů, které jsou oprávněny tato data vyžadovat, se jeví zcela nedostatečným a způsobuje v praxi vážné výkladové problémy. Přestože v původním legislativním návrhu se mělo jednat o Policii ČR a Vojenské zpravodajství, navrhl tehdejší Výbor pro obranu a bezpečnost vynětí zpravodajských služeb z tohoto zákona s tím, že jejich oprávnění budou specifikována později, a to v tzv. „protiteroristickém zákoně". K jeho přijetí však nikdy nedošlo, což po dobu několika let umožňovalo přístup k těmto datům pouze Policii ČR, resp. veškerým složkám majících status policejního orgánu dle ustanovení § 88a trestního řádu. To byla, obdobně jako hrazení nákladů ze strany států, opět zcela nestandardní a v Evropě výjimečná situace, což ze strany zpravodajských služeb vyvolalo snahy o obcházení zákona extenzivním výkladem předmětných ustanovení v zákoně o BIS.

Obdobně v případě odposlechů byla jako oprávněný orgán uvedena pouze Policie České republiky[49], což ale na rozdíl od data retention zásadní problém nezpůsobilo, a to z toho důvodu, že odposlechy pro zpravodajské služby byly do té doby realizovány prostřednictvím policie. Výslovné zmocnění požadovat po provozovatelích sítí zřízení rozhraní pro odposlech a záznam zpráv získaly BIS a Vojenské zpravodajství zákonem č. 290/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o Vojenském zpravodajství.

Zmocňovacím ustanovením v zákoně o elektronických komunikacích byla do právního řádu přijata dne 7. 12. 2005 vyhláška č. 485/2005 Sb.[50], která

[48] Podle § 97 odst. 6 zákona č. 127/2005 Sb., splnění povinností podle odstavců 1, 3, 4, náleží právnické nebo fyzické osobě od oprávněného subjektu, který si úkon vyžádal nebo jej nařídil, úhrada efektivně vynaložených nákladů. Výši a způsob úhrady efektivně vynaložených nákladů stanoví prováděcí právní předpis.
[49] Podle § 97 odst. 1 zákona č. 127/2005 Sb.
[50] Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávaní a formě a způsobu jejich předávání organům oprávněným k jejich využívání. Dostupné z: http://aplikace.mvcr.cz/sbirka- zakonu/ViewFile.aspx?type=c&id=4767

zpřesňovala rozsah údajů, které mají být uchovávány a předávány. Na podobě této vyhlášky pracovalo ještě tehdejší Ministerstvo informatiky ve spolupráci s Ministerstvem vnitra. S odstupem času lze říci, že požadavky na provozovatele telekomunikačních sítí byly nepřiměřeně tvrdé a plnění některých ustanovení, především v oblasti datového provozu, bylo technicky prakticky nemožné[51], což se rovněž později ukázalo v přímém porovnání se směrnicí 2006/24/ES.

S ohledem na skutečnost, že efektivně vynaložené náklady vzniklé v souvislosti se zajištěním ukládání a poskytování údajů bylo možné požadovat po žadateli, nevznikly v této oblasti žádné zásadní třecí plochy mezi veřejnou mocí a provozovateli telekomunikačních sítí, neboť některé náklady by se mohly pohybovat až v řádech miliard korun. Poněkud neobvyklé rovněž bylo ustanovení § 4 odst. 1 vyhlášky 485/2005 Sb., která explicitně stanovila dobu uchovávání těchto údajů na 6 měsíců, u serverových služeb pak na dobu 3 měsíců. V tomto světle se ustanovení zákona o elektronických komunikacích, které stanovovalo dobu uchovávání údajů na *„(…) dobu jejich uchovávání, která nesmí být delší než 12 měsíců,“*[52] jevilo jako poněkud zvláštní a nadbytečné a doposud nebyl ze strany státu vznesen požadavek na uchovávání informací na dobu delší 6 měsíců, tak jak stanovovala citovaná vyhláška.

3.4 Směrnice 2006/24/ES[53]

Jak bylo řečeno v předchozí kapitole, směrnice 2002/58/ES umožňovala členským státům přijmout opatření v zájmu národní bezpečnosti, spočívající, mimo jiné, v uchovávání údajů, avšak jednalo se pouze o právo každé země, a nikoliv její povinnost. Tato situace se však začala měnit vinou dalšího zostřování mezinárodní politické situace. Již po dalších teroristických útocích v Madridu v březnu 2004 vydala Evropská rada „Deklaraci pro boj s terorismem“[54] a zřídila pozici tzv. protiteroristického koordinátora EU. Specifické na madridském útoku z pohledu elektronických komunikací bylo, že se nejednalo o sebevražedný teroristický akt –

[51] Jednalo se především o povinnost monitorovat služby tzv.instant messengerů typu ICQ a IP telefonie, ustanovení bodů 3.3.5. přílohy k vyhlášce 485/2005 Sb.
[52] Podle § 97 odst.3, zák.č. 127/2005 Sb., o elektronických komunikacích.
[53] Směrnice Evropského parlamentu a Rady 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. [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:cs:PDF
[54] DECLARATION ON COMBATING TERRORISM. [online]. [cit. 2015-03-22]. Dostupné z: http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf

k vzdálenému odpálení náloží byla využita mobilní telefonní síť. Výsledkem této deklarace byl návrh „Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions,"[55] který se pokusil historicky poprvé stanovit provozovatelům elektronických komunikací povinnost uchovávat provozní a lokalizační údaje.

Zřejmě pod vlivem teroristických útoků byla navržena doba uchovávání těchto údajů v rozsahu 12 – 36 měsíců, přičemž především horní hranice této lhůty se jevila zcela nepřiměřená. O tom, že tento návrh byl poměrně nepřipravený, svědčí i to, že byl ze strany Evropského parlamentu i lidsko-právních organizací odmítnut pro porušení čl. 8 odst. 2 Evropské úmluvy o lidských právech[56]. Vůbec poprvé se tak ukázala obava z toho, že narušování soukromí, ke kterému by vlivem plošného uchovávání dat docházelo, by nebylo opatřením ultima ratio, ale stalo by se opatřením zcela běžným.

Dne 7. 7. 2005, tedy v době, kdy v České republice byl již účinný zákon o elektronických komunikacích, došlo k další vlně teroristických útoků, tentokrát na cíle v Londýně. To vyvolalo snahu o urychlené řešení poněkud roztříštěných přístupů k data retention v jednotlivých členských státech, a tak byla již 21. září 2005 představena Evropskou komisí nová směrnice[57], která měla dosud nejednotný právní rámec harmonizovat. Směrnice poté nabyla účinnosti 3. května 2006, tedy necelých 8 měsíců po útocích v Londýně. Směrnice obsahovala tyto hlavní povinnosti.

a) *Zajistit dostupnost údajů ze služeb elektronických komunikací, pro účely vyšetřování, odhalování a stíhání závažných trestných činů*[58]. Bohužel směrnice nijak nedefinuje pojem závažný trestný čin (v anglickém originále serious crime) a ponechává definici na národních právních řádech. Tento přístup později přinesl řadu aplikačních problémů.
b) *Stanovit kategorie údajů, které jsou členské státy povinny uchovávat*[59].

[55] Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions. [online]. [cit. 2015-03-22]. Dostupné z: http://www.statewatch.org/news/2002/aug/05datafd.htm
[56] Každý má právo na respektování soukromého a rodinného života, obydlí a korespondence
[57] Směrnice Evropského Parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/EC.
[58] Čl. 1 směrnice 2006/24/ES.
[59] Čl. 5 směrnice 2006/24/ES.

Rozsah povinných údajů byl menší než rozsah, který byli operátoři povinni uchovávat dle vyhlášky 485/2005 Sb. Dle směrnice nesmí být uchovávány žádné údaje odhalující obsah sdělení. Přesto, především v laických kruzích, je občas slyšet názor, že operátoři uchovávají obsah SMS zpráv.

c) *Povinnost členských států zajistit, aby se kategorie údajů uvedených v článku 5 uchovávaly po dobu nejméně 6 měsíců a nejdéle po dobu 2 let*[60].

Česká republika se, snad i z důvodů náhrady nákladů, přiklonila k nejkratší možné délce 6 měsíců.

d) Povinnost členských států zajistit, aby uchovávané údaje podléhaly stejnému zabezpečení a ochraně jako údaje na síti. Povinnost přijmout taková technická a organizační opatření, aby bylo zabráněno nepovolenému nebo neoprávněnému uchovávání, zpracování, přístupu nebo zveřejnění těchto dat, stejně jako zajištění přístupu k datům ze strany pouze oprávněných a zvlášť zmocněných osob. Na konci doby uchovávání údajů pak všechny údaje zničit, vyjma údajů, ke kterým bylo přistoupeno, a byly zajištěny[61].

V České republice je tato kontrola pravidelně realizována ze strany Českého telekomunikačního úřadu. Veškeré osoby, které zpracovávají tato data pro potřeby oprávněných orgánů, musí být prověřeny na minimální stupeň „Vyhrazené“, dle zákona 412/2005 Sb., o ochraně utajovaných informací.

e) Povinnost členských států zajistit, aby Komise jednou ročně obdržela statistiky o uchovávání údajů vytvořených nebo zpracovaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací.[62]

V článku 15 pak směrnice uložila členským státům povinnost uvést do souladu právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 15. září 2007. Rovněž stanovila, že co se týká údajů z připojení k internetu, internetové telefonie a internetové elektronické pošty, je možné

[60] Čl. 6 směrnice 2006/24/ES.
[61] Čl. 7 směrnice 2006/24/ES.
[62] Čl. 10 směrnice 2006/24/ES.

používání směrnice odložit do 15. března 2009. Česká republika se zavázala přijmout zákonnou úpravu do 36 měsíců od nabytí účinnosti směrnice.

3.5 Kontroverzní přijetí směrnice

Směrnice se prakticky ještě před svým vznikem stala terčem ostré kritiky většiny národních států. Především tzv. „pracovní skupina 29“, ustanovená na základě článku 29 směrnice 95/46/ES[63] a známá jako pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, navázala na své předchozí vyjádření[64] a ostře kritizovala plošnost tohoto opatření jako bezprecedentní zásah do lidských práv. Vyjádřila rovněž své obavy z porušení práva na soukromí a práva na informační sebeurčení. Jak již bylo řečeno dříve, obdobným způsobem se vyjádřil rovněž Peter Hustinx, Evropský inspektor osobních údajů, který tuto směrnici označil za nejinvazivnější zásah do soukromí, který kdy byl v EU přijat, co se týká rozsahu a množství osob, kterých se tato směrnice dotkne.[65]

Nejkomplexnější pohled pak podala oficiální hodnotící zpráva Evropské komise KOM (2011) 225[66]. Zásadní výhrady spatřovala Komise v následujících bodech:

a) Účelové omezení spočívající ve využívání dat jen pro účely stíhání závažných trestných činů se ukázalo jako nevyhovující, neboť přístup jednotlivých národních států k tomu, co je závažným trestným činem je zcela odlišný. Zatímco např. 10 členských států vymezilo pojem „závažný trestný čin“ na minimální dobu odnětí svobody, jiné členské státy vyžadovaly využití údajů pro všechny trestné činy.
b) Jednotlivé státy se liší v délce uchovávání různých typů údajů.

[63] Směrnice Evropského Parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046&from=CS

[64] Recommendation on the Respect of Privacy in the context of Interception of Telecommunications. [online]. [cit. 2015-03-22]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp18_en.pdf

[65] Hustinx: Data retention is the EU's most invasive tool. [online]. [cit. 2015-03-22]. Dostupné z: http://www.euractiv.com/infosociety/hustinx-data-retention-eus-invas-interview-504243

[66] Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES). [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52011DC0225&rid=2

c) Uchovávání údajů znamená významné omezení práva na soukromí.
d) Uchovávání údajů představuje poměrně významné náklady, které pro menší provozovatele mohou být značně zatěžující. Otázka hrazení nákladů státem je v Evropě výjimečná, a ve směrnici není řešena. Komise zváží způsoby poskytování konzistentních náhrad provozovatelům.

Bez ohledu na podstatné výhrady však Komise konstatovala, že pravidla EU o uchovávání údajů jsou nadále nezbytná pro policii, ochranu obětí a pro systémy trestní spravedlnosti. V této souvislosti nepostačuje pro vyšetřování trestné činnosti pouze tzv. zajišťování údajů, kdy je provozovatelům doručen soudní příkaz k zajištění údajů o konkrétních osobách, a to od data doručení tohoto příkazu, přestože není pochyb, že tento způsob zasahuje méně do soukromí, nežli plošné uchovávání informací o proběhnuvší komunikaci.

3.6 Oprávnění data vyžadovat

Jak již bylo uvedeno v předchozích kapitolách, potýkaly se provozovatelé sítí elektronických komunikacích kvůli chybějící či nepřesné legislativě s celou řadou problémů, komu a na základě jakého právního titulu uchovávaná data vůbec předávat. Přestože již zákon č. 151/2000 Sb., o telekomunikacích zaváděl ve svém § 84 odst. 7 povinnost tato data po dobu 2 měsíců uchovávat, ve svém odkazovacím ustanovení, které se týkalo toho, kdo je tedy oprávněn tato data vyžadovat zůstal vágní a nepřesný, neboť odkazoval pouze na speciální zákony, které byly uvedeny pod čarou, a to konkrétně na zákon č. 67/1992 Sb., Vojenské obranné zpravodajství, zákon č. 154/1994 Sb., Bezpečnostní informační služba a zákon č. 13/1993 Sb., Celní správa. V těchto zákonech však konkrétní zmocňovací zákonné ustanovení chybělo. Jako příklad lze uvést tehdejší ustanovení § 8 a § 9 zákona o BIS, ve kterém sice zákon hovořil o možném použití zpravodajské techniky po předchozím schválení předsedy senátu Vrchního soudu, ale nezmocňoval BIS k tomu, aby mohla požadovat vydání těchto dat po telekomunikačních operátorech. To samozřejmě vedlo ke značnému pnutí mezi BIS a operátory, neboť BIS zastávala názor, že k vyžádání dat postačovalo obecné zmocnění vyplývající se zákonného

ustanovení k používání zpravodajské techniky[67]. Operátoři nijak nezpochybňovali používání zpravodajské techniky, avšak, s ohledem na čl. 2 odst. 3 a odst. 4 Ústavy České republiky poukazovali na to, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon a nikdo nesmí být nucen činit, co zákon neukládá.

Obdobně neutěšená situace panovala rovněž ve vyžadování informací z telekomunikačního provozu ze strany Policie České republiky. Policie si tato data vyžadovala nejčastěji jako tzv. listinný důkaz dle ustanovení § 112 trestního řádu. Jako zcela nepřijatelné se pak jevily pokusy o vydání informací z telekomunikačního provozu na základě ustanovení § 8 odst. 1 trestního řádu, který se týkal obecné součinnosti fyzických a právnických osob. Průlomovým rozhodnutím v této věci se pak stal nález Ústavního soudu ÚS 502/2000 ze dne 22. 1. 2001. Stěžovatel, pravomocně odsouzený vrchním soudem za loupež v ústavní stížnosti namítal, že bylo porušeno jeho ústavně zaručené právo na spravedlivý proces garantované v článku 36 odst. 1 Listiny základních práv a svobod, neboť jako jeden z listinných důkazů byly použity výpisy telefonních hovorů, které byly získány, dle názoru stěžovatele, nezákonným způsobem[68].
Z obsahu spisů Ústavní soud zjistil, že (cituji):

„1) společnost Eurotel PRAHA, spol. s r. o., v dopise ze dne 7. 1. 1998 zaslala Policii ČR, Správě Středočeského kraje Praha, seznam hovorů, uskutečněných ve dnech 18. 6., 26. 8., 8. 10. a 25. 10. 1997, mj. z telefonu s t.č. 0602xxxxxx, včetně číselných kódů základových stanic, přes které byly hovory uskutečněny (č.l. 317a);

2) součástí spisu je seznam uskutečněných hovorů (č.l. 321), který obsahuje identifikační číslo telefonu, telefonní číslo volajícího (tj. 0602xxxxxx), datum a čas počátku hovoru, délku hovoru ve vteřinách, číslo základové stanice, kde hovor započal, a číslo základové stanice, kde byl hovor ukončen;

3) uvedená společnost zaslala dopis ze dne 17. 4. 1998 Policii ČR, Krajskému úřadu vyšetřování Praha, ze kterého vyplývá, že držitelem telefonu s t.č. 0602xxxxxx je stěžovatel (č.l. 309-309a);

[67] Zpravodajskou technikou se pro účely tohoto zákona rozumějí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické, anebo jejich soubory, používané utajovaným způsobem při: odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního provozu a jiného obdobného provozu.
[68] Nález Ústavního soudu ÚS 502/2000 ze dne 22. 1. 2001. [online]. [cit. 2015-03-22]. Dostupné z: http://kraken.slv.cz/II.US502/2000

4) jak vyplývá ze svědecké výpovědi Ing. H. K., zaměstnankyně společnosti Eurotel PRAHA, učiněné u hlavního líčení (č.l. 748 a násl.), na jejího zaměstnavatele se obrátil zvláštní technický útvar kriminální policie, který souhrnně zadává požadavky, přičemž uvedená společnost oprávněnost těchto požadavků neověřuje; na základě toho byly zpracovány seznamy hovorů; odpověď datovaná lednem 1998 byla zaslána na žádost centrální složky policie na adresu složky, která byla uvedena v žádosti, přičemž již v roce 1997 byly v dané věci poskytovány informace minimálně dvakrát.“ [69]

Ústavní soud na základě těchto zjištění konstatoval, že bylo porušeno právo na ochranu zpráv podávaných telefonem plynoucí z článku 13 LZPS jako ústavně zaručené právo, které svou povahou a významem patří mezi základní lidská práva a svobody. Součástí ústavní ochrany je pak nejen vlastní obsah přenášených zpráv, ale rovněž údaje vztahující se k přenášené zprávě, tedy právě ty, které byly společností Eurotel poskytnuty. Dále konstatoval, že „*současná právní úprava nezná institut poskytování či pořizování evidence telekomunikačního provozu pro účely trestního stíhání či plnění úkolů policie (či institut jinak nazvaný, ale obsahově shodný). Neznamená to však, že by příslušné státní orgány nebyly oprávněny za žádných okolností tuto evidenci pořizovat či vyžadovat. S ohledem na to, že jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany těchto orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto ‘dalších, údajů, tj. při evidování telekomunikačního provozu. Orgány činné v trestním řízení, resp. policejní orgány před zahájením trestního stíhání, jsou tedy v případě pořizování či získávání evidence telekomunikačního provozu povinny postupovat přiměřeně podle § 88 trestního řádu, resp. podle § 36 zákona č. 283/1991 Sb., o Policii ČR, ve znění pozdějších předpisů, a to tak, že pojem ‘záznam, se vztahuje také na údaje získané evidováním telekomunikačního provozu ve vztahu ke konkrétní osobě nebo osobám.“*[70]

Ústavní soud rozhodl, že zařazení těchto listinných důkazů do spisu je nejen nezákonné, ale navíc ústavně zcela nepřijatelné. Dalšími obdobnými nálezy pak byly nálezy ÚS 536/2000[71] nebo IV. ÚS 78/01[72].

[69] ÚS 502/2000. [online]. [cit. 2015-03-22]. Dostupné z: http://kraken.slv.cz/II.US502/2000
[70] ÚS 502/2000. [online]. [cit. 2015-03-22]. Dostupné z: http://kraken.slv.cz/II.US502/2000
[71] ÚS 536/2000. [online]. [cit. 2015-03-23]. Dostupné z: http://kraken.slv.cz/IV.US536/2000
[72] ÚS 78/01. [online]. [cit. 2015-03-23]. Dostupné z: http://kraken.slv.cz/IV.US78/01

Jak se později ukázalo, ani ustanovení § 88 trestního řádu, který se využíval pro odposlech a záznam telekomunikačního provozu a jako takový jej bylo možné použít jen po nařízeném soudním příkazu či se souhlasem uživatele odposlouchávané telefonní stanice, nebylo z hlediska ústavní konformity dostatečné a zákonodárce musel přijmout novou právní úpravu[73].

Tato nová právní úprava byla přijata společně s velkou rekodifikací trestního řádu, ke které došlo zákonem č. 265/2001 Sb.[74] ze dne 31. 7. 2001. Rekodifikací byl do trestního řádu zaveden § 88a, který jasně oddělil institut odposlechů od institutu vyžadování provozních a lokalizačních údajů. Osoby vykonávající telekomunikační činnost byly povinny na základě písemně vydaného a odůvodněného příkazu předsedy senátu či soudce (v přípravném řízení) vydat tyto údaje státnímu zástupci nebo policejnímu orgánu, přičemž pod pojem policejní orgán byly zařazeny všechny orgány taxativně vyjmenované v ustanovení § 12 odst. 2 trestní řádu.

Jedinou možností, jak se lze soudnímu přezkumu požadavku na vydání těchto dat vyhnout zůstává využití souhlasu uživatele telekomunikačního zařízení, ke kterému se mají tyto údaje vztahovat. To se však v praxi jeví v některých případech jako poměrně obtížně aplikovatelné, neboť především právnické osoby, ale i mnohé fyzické osoby mají na své jméno registrováno více SIM karet a není tak zcela zřejmé, zda právě oni jsou uživatelem dotčeného zařízení, nebo to je např. manželka či zaměstnanec právnické osoby. Kromě tohoto ustanovení umožňuje trestní řád v § 158d trestního řádu získávat poznatky o osobách a věcech v rámci tzv. sledování osob a věcí, prováděného utajovaným způsobem technickými nebo jinými prostředky. Tento institut však nelze zaměňovat s institutem data retention, neboť takové sledování se děje od doby soudního povolení směrem do budoucnosti, a nikoliv směrem k datům získaným v rámci povinného uchovávání údajů 6 měsíců zpětně. Svou charakteristikou je tak blíže spíše institutu „zajišťování údajů“, který byl popsán v kapitole 3.5. Ať se však jedná o institut vyžadování údajů, či zajišťování údajů, oba podléhají soudnímu přezkumu zákonnosti a rovněž parlamentní kontrole ústavnosti. Poslanecká sněmovna zřídila k tomuto účelu kontrolní orgán, kterým je Stálá poslanecká komise pro kontrolu použití odposlechu

[73] Viz např. rozsudek ve věci Heglas vs. Česká republika, kapitola 2.4.3.
[74] Zákon č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, a některé další zákony. [online]. [cit. 2015-03-23]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=265&r=2001

a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací.[75] V současné právní úpravě však bohužel existuje institut, který takového kontrole nepodléhá (viz kapitola 3.6.1).

3.6.1 Oprávnění dle § 66 zák. č. 273/2008 Sb.

Zákon č. 273/2008 Sb., o Policii České republiky umožňuje policii ve svém ustanovení § 66 odst. 3 týkající se informací z evidencí v *„případech stanovených zákonem a v rozsahu potřebném pro plnění konkrétního úkolu žádat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis[76] jinak. Tyto osoby jsou povinny žádosti vyhovět bez zbytečného odkladu, ve formě a v rozsahu stanoveném jiným právním předpisem.“*[77] Konkrétně je pak toto oprávnění specifikováno v ustanovení § 68 odst. 2, podle kterého je policie oprávněna žádat tyto údaje *„(…) pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly.”*[78] Tyto údaje může policie vyžadovat způsobem, který umožňuje dálkový a nepřetržitý přístup. V praxi je dálkový přístup realizován tak, že policie zašle operátorovi příkaz k aktivaci odposlechu konkrétního zájmového čísla, avšak bez obsahu příslušné komunikace.[79] Policejnímu orgánu jsou pak automaticky odesílána pouze data o uskutečněné komunikaci, avšak nikoliv obsah této komunikace. Zásadně problematickou se jeví absence jakékoliv soudní či parlamentní kontroly a také skutečnost, že tato data jsou vyžadována mimo oblast trestního řízení, kdy trestní spis je automaticky dozorován státním zástupcem. Obdobně problematickým je pak § 71 zákona o Policii ČR, kdy:

„Útvar policie, jehož úkolem je boj s terorismem, může za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu v nezbytném rozsahu žádat od:

---

[75] Členové - Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací. [online]. [cit. 2015-03-23]. Dostupné z: http://www.psp.cz/sqw/snem.sqw?id=1139

[76] Zákon č.127/2005 Sb., o elektronických komunikacích.

[77] Podle § 66 odst. 3 zákona č. 273/2008 Sb., o Policii České republiky.

[78] Podle § 68 odst. 2 zákona č. 273/2008 Sb., o Policii České republiky.

[79] Většina odposlechových systému umožňuje navolit typ dat, která mají být zasílána žadateli. Jedná se buď pouze o doprovodná data, tedy např. místo, čas, délka komunikace, spojované číslo apod. Nebo rovněž i o obsah komunikace. Tento obsah lze dále rozdělit na obsah hlasové komunikace a obsah datových paketů.

a) *právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak; informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem*[80]*,*

b) *banky předávání dat o době a místě použití elektronického platebního prostředku,*

c) *zdravotní pojišťovny nebo poskytovatele zdravotních služeb* poskytnutí informací o době a místě poskytnutí zdravotních služeb.“[81]

Na skutečnost, že podobné ustanovení zákona je z hlediska ochrany provozních a lokalizačních údajů, ke kterému jsou operátoři zavázáni, velmi problematické, upozorňují nejen samotní operátoři, ale rovněž i občanská sdružení typu Iuridicum Remedium, která tato ustanovení dlouhodobě ostře kritizují[82]. Při jednáních s kompetentními osobami na straně Policejního prezidia jsou všechny strany ujišťovány, že policie má vlastní, údajně velmi přísné kontrolní mechanismy, díky kterým je zneužití tohoto institutu prakticky vyloučeno. O tom lze mít určité pochybnosti, neboť v minulosti bylo zaznamenáno několik případů, kdy si policisté při vyšetřování trestné činnosti nechali prostřednictvím soudů schvalovat příkazy k vydání provozních a lokalizačních údajů, přičemž mezi telefonní čísla důvodně podezřelých podsunuli vždy čísla telefonů, na jejichž výpisech měli vlastní zájem. Bohužel v případě, kdy jsou podezřelých desítky, je pro příslušný soud velmi obtížné zabývat se vztahy mezi telefonními čísly a konkrétním případem. Za mediálně „nejslavnější“ je pak možné označit smutný příběh bývalého policisty Mariana Hudce, který tímto způsobem nezákonně zjišťoval údaje z telekomunikačního provozu více než 40 významných osobností, mimo jiné např. i údaje z mobilního telefonu tehdejšího předsedy Ústavního soudu Pavla Rychetského[83].

---

[80] Zák. č. 127/2005 Sb. o elektronických komunikacích.
[81] Podle § 71 zák. č. 273/2008 Sb., o policii České republiky.
[82] VOBOŘIL, Jan. Výhrady o.s. Iuridicum Remedium proti návrhu novely zákona o elektronických komunikacích a některých dalších zákonů upravujících povinnost uchovávat provozní a lokalizační údaje o elektronických komunikacích a způsoby využívání těchto údajů (sněmovní tisk č. 383). [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/vyhrady_-_senatni_tisk_c._383_-_monitorovani_provoznich_a_lokalizacnich_udaju_o_elektronicke_komunikaci.pdf
[83] Policista, který šmíroval politické špičky, dostal podmínku. [online]. [cit. 2015-03-23]. Dostupné z: http://tn.nova.cz/clanek/zpravy/domaci/policista-ktery-smiroval-politicke-spicky-dostal-podminku.html

Přestože § 88a přinesl do právního řádu tolik potřebné zakotvení institutu data retention a především pak jeho oddělení od odposlechů, ukázalo se, že stále nebyl tento institut brán tak vážným způsobem jako samotné odposlechy. Jak je popsáno výše, je totiž možné se k těmto informacím dostat částečně i mimo soudní či parlamentní kontrolu. Stejně tak i prostým porovnáním s tehdejším, přísným ustanovením § 88 o podmínkách nařízení odposlechu, zjistíme, že toto ustanovení taxativně stanovuje, u jakých trestných činů připadá nařízení odposlechu v úvahu, zatímco v ustanovení § 88a se zákonodárci spokojili s nedostatečným a extrémně širokým vymezením spočívajícím v konstatování, že k poskytnutí výpisu postačí, je-li to třeba k objasnění skutečností důležitých pro trestní řízení. V praxi pak takovéto vymezení muselo samozřejmě vést k tomu, že tento institut byl nadužíván, neboť vydání informací o telekomunikačním provozu bylo vyžadováno často i u bagatelních trestných činů. To ostatně potvrdila i v dřívějších kapitolách citovaná zpráva Evropské komise KOM (2011) 225. Ta konstatuje, že v České republice bylo v roce 2008 vydáno celkem 131.560 žádostí o poskytnutí informací o proběhnuvším telekomunikačním provozu a v roce 2009 dokonce 280.271, což představuje více než 100% nárůst. Je zřejmé, že nadužívání významně neomezilo ani povinné hrazení nákladů na poskytování těchto údajů ze strany státu, ale spíše až budoucí ostrá společenská kritika a změna právních předpisů, ke které došlo po ústavním nálezu PL ÚS 24/10, který bude podrobněji rozebrán v kapitole 5.4.

3.7 Aktuální právní úprava oprávnění data vyžadovat

Po zmiňovaném nálezu Ústavního soudu, který bude detailně analyzován v následujících kapitolách, došlo prostřednictvím zákona 273/2012 Sb.[84], k rozsáhlé novelizaci příslušných ustanovení zákona o elektronických komunikacích, které se týkaly orgánů oprávněných data z telekomunikačního provozu vyžadovat. V § 97 odst. 3 byly nově taxativně vyjmenovány všechny tyto oprávněné orgány:

- **Orgány činné v trestním řízení** za podmínek uvedených v trestním řádu.
- **Policie České republiky** pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé

[84] Zákon č. 273/2012 Sb., zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

totožnosti, či totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby.

- **Bezpečnostní informační služba**
- **Vojenské zpravodajství**
- **Česká národní banka**

Současně byly novelizovány veškeré speciální zákony, které se vztahují k vyjmenovaným subjektům tak, aby výklad byl jednotný a bezrozporný. Především BIS přijala zmiňovanou právní úpravu s velkou úlevou, neboť do té doby ji operátoři odmítaly tato data vydávat, a to i přesto, že BIS byla přesvědčena, že na vydání dat má právní nárok[85] (viz kapitola 3.3). S velkými rozpaky pak byla odbornou veřejností přijata skutečnost, že mezi oprávněnými subjekty se objevila Česká národní banka. V kontextu ostatních centrálních bank členských států se jedná o oprávnění zcela ojedinělé. S ohledem na to, že od nabytí účinnosti tohoto oprávnění společnost T-Mobile neřešila ze strany ČNB žádný požadavek na vydání těchto údajů, tak zřejmě i nadbytečné. Jak uvádí Jan Vobořil[86], jedná se o implementaci směrnice Evropského parlamentu a Rady 2003/6/ES, čl. 12, odst. 2, písm. d) o zneužívání trhu. V českém právním řádu pak chybí implementace odst. 3 tohoto článku, který stanovuje, že má být šetřeno profesní, tedy i telekomunikační tajemství.

[85] Operátorům nic nedlužíme a nové pravomoce nechceme. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bis.cz/n/2005-03-22-operatorum-nic-nedluzime-a-nove-pravomoce-nechceme.html

[86] VOBOŘIL, Jan. Výhrady o.s. Iuridicum Remedium proti návrhu novely zákona o elektronických komunikacích a některých dalších zákonů upravujících povinnost uchovávat provozní a lokalizační údaje o elektronických komunikacích a způsoby využívání těchto údajů (sněmovní tisk č. 383). [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/vyhrady_-_senatni_tisk_c._383_-_monitorovani_provoznich_a_lokalizacnich_udaju_o_elektronicke_komunikaci.pdf

4 Úhrada nákladů za poskytování informací

4.1 Stav před nabytím účinnosti zákona o elektronických komunikacích

Plnění zákonných povinností spojených s odposlechy či uchováváním provozních a lokalizačních údajů je pro provozovatele sítí spojeno s nemalými náklady. V případě odposlechů se navíc jedná o nákup hardwaru, který nelze využít žádným jiným způsobem v síti operátora, ale slouží výhradně k plnění zákonných povinností. Investiční náklady na vybudování infrastruktury se pohybují v řádech desítek milionů korun. Nelze opomenout rovněž náklady provozní, a to jak ve smyslu údržby této infrastruktury, tak i ve smyslu personálním, tedy nákladů na mzdy a vybavení zaměstnanců, kteří se vyřizováním požadavků zabývají. U provozních a lokalizačních údajů je situace pro provozovatele o něco příznivější.

Každý operátor uchovává pro potřeby řádného vyúčtování či vyřízení reklamací informace o uskutečněných hovorech nebo proběhnuvších datových paketech, tedy informace, které nutně potřebuje při výkonu své podnikatelské činnosti[87]. Tyto údaje však uchovává podstatně kratší dobu a poté, co jich již není třeba je povinen je zlikvidovat. Rovněž rozsah údajů, které operátor potřebuje k řádnému vyúčtování, je mnohem užší. V době účinnosti zákona o telekomunikacích[88] zajišťoval operátor plnění těchto povinností na své vlastní náklady. To v případě data retention nepředstavovalo extrémní zátěž, neboť jak již bylo řečeno, operátor většinu těchto dat stejně potřeboval ke své podnikatelské činnosti (na rozdíl od odposlechů) a dle zákona o telekomunikacích musel tato data uchovávat pouze 2 měsíce. Přesto se v Evropě v letech 2004 a 2005 začaly ozývat kritické hlasy upozorňující na skutečnost, že díky postupnému zavádění tzv. flateových tarifů, které spočívají v nabídce neomezeného volání a dat za fixní cenu, nebudou v budoucnu muset operátoři tato data uchovávat vůbec, neboť zákazník jednoduše zaplatí jednu cenu za de facto neomezenou službu. To se však v této době netýká České republiky a ani osobně tento názor nesdílím. Po atentátech v Madridu a Londýně, jak již bylo řečeno v předchozích kapitolách, začaly probíhat diskuse o nutnosti sjednotit rozsah uchovávaných údajů, stejně jako prodloužit dobu uchovávání, či zavést alespoň minimální dobu uchovávání těchto údajů.

[87] Podle § 90, § 91 zákona č. 127/2005 Sb., o elektronických komunikacích.
[88] Zákon č. 151/2000 Sb.

V atmosféře zjitřené teroristickými činy nebyly výjimečné ani názory požadující uchovávání těchto údajů po dobu 36 měsíců, což by pro operátory znamenalo, s ohledem na objem dat z internetového provozu, náklady přímo extrémní. O to větším překvapením pak bylo, že zákonodárci zavedli v novém zákoně o elektronických komunikacích mechanismus zajišťující náhradu efektivně vynaložených nákladů státem.

4.2 Úhrada nákladů po nabytí účinnosti zákona o elektronických komunikacích

Zákon č. 127/2005 Sb., o elektronických komunikacích zavedl povinnost státu hradit provozovatelům elektronických komunikací investiční a provozní náklady vzniklé v souvislosti s uchováváním a poskytováním těchto údajů. Zmocňovacím ustanovením zákona byly delegovány povinnosti vydání prováděcího podzákonného právního předpisu na Český telekomunikační úřad. Přes velkou snahu se nepodařilo vydat tento předpis až do 7. 12. 2005, kdy jej ČTÚ vydal vyhlášku č. 486/2005 Sb.[89] (dále jen nákladová vyhláška). Tato vyhláška umožnila provozovatelům elektronických komunikací požadovat úhrady za následující množiny výdajů.

a) *Náklady na zřízení a zabezpečení rozhraní pro připojení zařízení pro odposlech a záznam zpráv*[90].

   Operátorům tak mohly být vyplaceny náklady spojené s koupí hardwaru a vybudování příslušné infrastruktury a přenosových tras týkající se odposlechů. Operátorům nepřísluší náhrada nákladů spojených s aktivací, deaktivací, či modifikací zájmové adresy (nejčastěji telefonní číslo), tedy úhrady spojené se zaměstnanci operátora, kteří požadavky oprávněných subjektů řeší. Český telekomunikační úřad však přesto vložil do ustanovení § 1 nákladové vyhlášky omezující prvek, který zabraňuje tomu, aby stát nebyl nucen jednorázově uhradit extrémní náklad. Úhrada totiž přísluší operátorům pouze ve formě tzv. měsíčních účetních odpisů

[89] Vyhláška č. 486/2005 Sb., kterou se stanoví výše a způsob úhrady efektivně vynaložených nákladů na zřízení a zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby. [online]. [cit. 2015-03-23]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=486&r=2005

[90] Podle § 1 vyhlášky 486/2005 Sb.

pořízeného zařízení dle zákona č. 563/1991 Sb., o účetnictví. V praxi to znamená, že jednorázově vydaný náklad ze strany operátora, mu bude splácen dle příslušné odpisové doby, u tohoto typu hardware zpravidla desetileté.

b) *Výše nákladů na uchovávání provozních a lokalizačních údajů*[91].
Nyní se již dostáváme do oblasti data retention, kde operátorům, obdobně jako u odposlechů, náleží formou měsíčních účetních odpisů zařízení veškeré náklady, které byly efektivně vynaloženy v souvislosti s uchováváním těchto údajů. Nejčastěji se jedná o datová úložiště a servery, které tato data zpracovávají a exportují do podoby, ve které jsou předávána oprávněným subjektům. Operátor samozřejmě musí oprávněnému subjektu prokázat, že se skutečně jedná o náklady, které by jinak operátorům nevznikly, neboť operátor sám řadu těchto údajů uchovává a zpracovává při zajišťování podnikatelské činnosti. Vzhledem ke komplexnosti IT a NT (network technoligies) systémů je to často velmi obtížné.

c) *Výše nákladů na poskytování provozních a lokalizačních údajů*[92].
Tato výše nákladů byla ze strany ČTÚ stanovena formou přílohy nákladové vyhlášky, kde je každý úkon ze strany operátora finančně ohodnocen. Vyhláška navíc rozděluje to, zda se jedná o úkon, který byl vyžádán prostřednictvím dálkového přístupu, a tedy zpracován do značné míry automatizovaně, nebo v listinné podobě, kdy je náklad operátora vyšší. Pro lepší představu, běžný výpis telekomunikačního provozu za dobu nepřesahující 60 dní byl v této vyhlášce oceněn na částku 32,- Kč při vyžádání prostřednictvím dálkového přístupu.

d) *Výše nákladů na poskytnutí informace z databáze účastníků*[93].
Jedná se o náklady vynaložené se zjištěním a identifikací účastníka, či jiného identifikátoru v síti operátora. Obdobně jako v předchozím

[91] Podle § 2 vyhlášky 486/2005 Sb.
[92] Podle § 2 vyhlášky 486/2005 Sb.
[93] Podle § 3 vyhlášky 486/2005 Sb.

případě byla tato částka stanovena taxativně, přílohou nákladové vyhlášky.

Sdružení Iuridicum Remedium (IuRe) ve svém vyjádření *„Data retention v (nejen) policejní praxi,“*[94] uvádí tabulku celkových nákladů vyplacených ze strany Policie ČR všem operátorům, kteří úhradu nákladů řádným způsobem uplatnili. Celková výše nákladů, kterou operátorům poskytly ostatní subjekty, se nebude příliš lišit, neboť policie vyžaduje zdaleka největší množství informací. Tyto náklady získaly zástupci IuRe na schůzce se zástupci Policie České republiky, Útvarem zvláštních činností dne 1. 6. 2012 (viz Tabulka č. 1).

Tabulka č. 1: Tabulka vynaložených nákladů na poskytování provozních a lokalizačních údajů.

Rok	2009	2010	2011
Provozní náklady	37.954.990,- Kč	39.736.536,- Kč	20.431.464,- Kč
Investiční náklady	146.693.103,- Kč	124.789.242,- Kč	91.220.706,- Kč
Celkem	184.648.093,- Kč	164.525.778,- Kč	111.652.170,- Kč

(Zdroj: Data retention v (nejen) policejní praxi. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf)

Z přiložené tabulky je patrné, že se nejedná o nijak zanedbatelnou položku ve státním rozpočtu, a proto se úhrada nákladů stává pravidelným tématem politiků usilujících o zrušení tohoto mechanismu a návrat před rok 2005, kdy veškeré náklady na svých bedrech neslï operátoři. Je také zřejmé, že postupně dochází ke snižování nákladů, což však lze přičíst spíše postupnému ukončování odpisových lhůt jednotlivých hardwarových či softwarových prvků, nežli razantnímu snižování počtu požadavků, i když i tam ke snížení po celospolečenské debatě došlo.

Vyhláška 462/2013 Sb.,[95] pak nákladovou vyhlášku novelizovala. Důvodem byly některé změny, ke kterým došlo ve spolupráci mezi oprávněnými subjekty a operátory. Operátorům se totiž podařilo, po dohodě s oprávněnými

[94] Data retention v (nejen) policejní praxi. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf

[95] Vyhláška č. 462/2013 sb., 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. [online]. [cit. 2015-03-23]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=462&r=2013

subjekty, podstatným způsobem automatizovat vyřizování zákonných požadavků, avšak v předchozí vyhlášce absentovalo ustanovení, které by umožňovalo takovéto vícenáklady operátorům zaplatit. Je pochopitelné, že snížení podílu „ruční práce“ ze strany operátora vedlo rovněž k přehodnocení taxativně uvedených částek za jednotlivé úkony uvedené v příloze této vyhlášky. A tak, jak bylo uvedeno výše, poskytnutí výpisu hovorů nepřesahující dobu 60 dní bylo ohodnoceno částkou 32,- Kč. Nyní je to již jen 19,- Kč.

4.3 Zhodnocení ústavní konformity úhrady nákladů

Úhrada nákladů tak, jak byla do právního řádu České republiky zavedena, je v evropském kontextu poměrně výjimečná. Dle již několikrát citované zprávy Evropské komise, provozní a investiční náklady nahrazovaly operátorům kromě České republiky jen Velká Británie a Finsko. Belgie, Dánsko, Estonsko, Litva, Nizozemsko a Francie pak nahrazují pouze náklady provozní, ostatní státy pak nenahrazují žádné výdaje nebo žádné relevantní údaje Evropské komisi neposkytly. To bohužel vede ke smutnému pravidlu, že téměř pokaždé, když se mění politická reprezentace země, probíhají politické diskuse o tom, zda s ohledem na tristní stav veřejných rozpočtů tuto úhradu nezrušit.

To by však, dle mého názoru, bylo v rozporu s ústavním pořádkem. Dle článku 11 odst. 1 Listiny základních práv a svobod je zakotveno právo na vlastnictví majetku, přičemž vlastnická práva všech vlastníků mají stejný zákonný obsah a ochranu. Dle článku 11 odst. 4 je pak možné vyvlastnění či nucené omezení vlastnického práva jen při splnění tří kumulativních podmínek, tedy jen ve veřejném zájmu, na základě zákona a za náhradu. V tuto chvíli jsou všechny tyto podmínky splněny, neboť legitimním veřejným zájmem státu je boj proti kriminalitě či terorismu a tohoto účelu nelze bezezbytku dosáhnout vyloučením odposlechů či data retention. Druhá podmínka, tedy zákonnost takového opatření, je rámována nejen českou legislativou, ale rovněž i legislativou evropskou (před zrušením směrnice, viz dále).

Třetí podmínka je rovněž splněna, i když lze pochopitelně diskutovat o tom, zda je tak učiněno plně uspokojivým způsobem. To se týká především účetních odpisů zařízení, kdy operátor vydává jednorázový náklad v čase pořízení a tato investice je mu poté hrazena několik let. Aktuální úprava tak nezohledňuje hodnotu peněz v čase a operátor poskytuje státu jakousi bezúročnou, víceletou půjčku.

Obdobně není ze strany státu hrazen operativní náklad u odposlechů, spočívající v manuálním zadávání požadavků ze strany pověřených zaměstnanců. Na druhou stranu jsou ze strany státu hrazeny veškeré náklady spojené s vyřizováním požadavků na data retention, přičemž tyto náklady, s ohledem na značný stupeň automatizace, pokrývají náklady operátora beze zbytku, či spíše dokonce ekonomicky přínosným způsobem. Lze tedy konstatovat, že celková výše nákladů je ze strany státu plně hrazena.

S ohledem na značnou výši nákladů, kterou operátor musí v souvislosti se zajištěním povinností (odposlech a data retention) zajistit, je zřejmé, že pokud by v budoucnu došlo ke zrušení hrazení nákladů ze strany státu, jednalo by se s největší pravděpodobností o krok protiústavní, neboť by se podstatně omezilo právo vlastníka věc užívat - ius utendi, či s ní nakládat - ius disponendi.

5 Ústavnost směrnice o data retention 2006/24/ES

Jak již bylo uvedeno v kapitolách 3.4. a 3.5, nesetkala se směrnice o uchovávání údajů 2006/24/ES v Evropě s nijak vřelým přijetím. Transpoziční doba byla členským státům určena do 15. září 2007, v případě internetového provozu pak do 15. března 2009. Některé členské státy již v té době měly vlastní národní úpravy, včetně České republiky. Národní úprava byla v České republice svým rozsahem uchovávaných údajů[96] přísnější, než samotná evropská směrnice. Kritické přijetí vedlo k tomu, že řada států podrobila tuto směrnici ústavněprávnímu přezkumu. Některá rozhodnutí soudů si představíme v následujících kapitolách.

5.1 Bulharsko

Státní agentura pro informační technologie a komunikace a ministerstvo vnitra implementovaly tuto směrnici nařízením, přičemž toto nařízení stanovovalo operátorům povinnost uchovávat provozní a lokalizační údaje po dobu 12 měsíců. Jako problematická se ukázala možnost přímého přístupu zpravodajských služeb k požadovaným údajům, a to bez soudního přezkumu, stejně jako přístup ministerstva vnitra přes tzv. pasivní počítačový terminál (čl. 5 nařízení). V průběhu roku 2008 se tak, díky lidsko-právním organizacím, dostala k Nejvyššímu správnímu soudu Bulharska stížnost na implementaci této směrnice. Ta poukazovala na zjevný rozpor s článkem 8 Evropské úmluvy o lidských právech. Přestože v první instanci byla stížnost dne 17. července 2008 zamítnuta, při odvolání pak pětičlenný senát nejvyššího správního soudu označil shora uvedený přístup k údajům za neústavní a dne 11. prosince 2008 bylo nařízení zrušeno[97]. Příčinu neústavnosti spatřoval soud ve skutečnosti, že (cituji): *„Článek 5 nařízení není dostatečně jasný, pokud jde o ochranu práva na respektování soukromého a rodinného života, což je v rozporu s ustanovením čl. 8 EÚLP, znění směrnice 2006/24/ES, a práva na ochranu soukromého života a korespondence dle článků 32 a 34 bulharské ústavy.“*[98]

[96] Podle § 97 zákona č. 127/2005 Sb. o elektronických komunikacích a Vyhláška 485/2005 Sb., o uchovávání provozních a lokalizačních údajů.
[97] Bulgarian Court Annuls A Vague Article Of The Data Retention Law. [online]. [cit. 2015-03-23]. Dostupné z: http://history.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention
[98] Ústava Bulharské republiky (dostupná v anglickém jazyce). [online]. [cit. 2015-03-23]. Dostupné z: http://www.parliament.bg/en/const

5.2 Rumunsko

Obdobně jako v Bulharsku, tak i v Rumunsku se o iniciaci ústavního přezkumu zasloužily lidsko-právní organizace. Napadeným se stal zákon č. 298/2008. Stěžovatelé poukázali na rozpor směrnice s články rumunské ústavy[99] č. 25, 26, 28 a 30, které zaručují právo svobody pohybu, rodinného a osobního života, ochranu listovního tajemství a svobody projevu. Rumunský ústavní soud poukázal na citlivé vyvážení individuálních a ústavních práv člověka a zájmy společnosti, nicméně konstatoval, že omezení vyplývající z aplikace směrnice mohou být ospravedlnitelná, výhradně za striktních podmínek daných jak článkem 8 Evropské úmluvy o lidských právech, tak i článkem 53 rumunské ústavy. Tyto pojistky by měly být ochranou před svévolným přístupem veřejné moci. Neurčitost a nedostatečně vymezený průnik této směrnice do soukromí přináší dle názoru ústavního soudu možnost tato data zneužít.

Rumunský soud se také překvapivě vymezil proti samotnému držení těchto údajů. Konstatoval, že běžným stavem ve společnosti je zasahovat do ústavně zaručených práv pouze výjimečně, zatímco plošné uchovávání těchto údajů ve stanoveném rozsahu a délce znamená úplné popření tohoto principu, neboť data jsou uchovávána o každém, bez ohledu na to, zda se konkrétní občan dopustil páchání trestné činnosti či terorismu. Z tohoto důvodu označil příslušný zákon za protiústavní[100] a dne 8. října 2009 jej zrušil.

5.3 Německo

Občanská iniciativa AK VORRAT[101] iniciovala ústavní stížnost u Spolkového ústavního soudu již na konci roku 2007. Cílem stížnosti se staly § 113a a § 113b německého telekomunikačního zákona. Zatímco § 113a ukládal povinným subjektům ukládat data po dobu 6 měsíců, § 113b pak stanovil rozsah jejich využití. Stejně tak bylo napadeno ustanovení § 100g trestního řádu, který upravoval využívání těchto dat v rámci trestního řízení. Stěžovatelé poukazovali na

[99] Ústava Rumunské republiky (dostupná v anglickém jazyce). [online]. [cit. 2015-03-23]. Dostupné z: http://www.cdep.ro/pls/dic/site.page?id=371
[100] Rozhodnutí č. 1258. [online]. [cit. 2015-03-23]. Dostupné z: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf
[101] SPD-Zustimmung zur Vorratsdatenspeicherung wäre Betrug am Wähler. [online]. [cit. 2015-03-23]. Dostupné z: http://www.vorratsdatenspeicherung.de/

to, že napadená ustanovení porušují čl. 10 Základního zákona (Grundgesetz)[102] chránící důvěrnost komunikací. Součástí stížnosti byl rovněž návrh na předložení předběžné otázky k Soudnímu dvoru EU. Tato předběžná otázka měla řešit, zda samotná směrnice není v rozporu s unijním právem a nepředstavuje zásah do základních lidských práv. To však spolkový ústavní soud odmítl s argumentací, že směrnice stanovuje dostatečné mantinely k jejímu provedení takovým způsobem, který bude respektovat ústavně zaručená práva a svobody.

V článku 10 Grundgesetz se však Spolkový ústavní soud s názorem stěžovatele ztotožnil. Při svém zkoumání legality, legitimity a proporcionality sledovaného cíle konstatoval, že především v otázce proporcionality, zahrnující plošné a preventivní ukládání údajů je německá úprava ústavně nekonformní. Zároveň poukázal na fakt, že uchovávaná data by měla být zabezpečena pod hrozbou sankcí nadstandardním způsobem, který bude minimalizovat rizika jejich zneužití, což současná ustanovení negarantují. Z těchto důvodů byla účinnost napadených ustanovení pozastavena v březnu 2010. Zároveň soud provozovatelům nařídil veškerá získaná data okamžitě smazat[103].

Obdobně komplikovaného přijetí se směrnice data retention setkala i v mnoha dalších členských státech, a to na Kypru, ve Slovensku, v Maďarsku, v Polsku či ve Švédsku, kde byla příslušná transpoziční ustanovení (či jejich části) buď zrušena, nebo byla ústavními soudy projednávána[104]. Později však přece jen došlo v otázce přijímání směrnice data retention k radikální změně, která byla vyvolána společným řízením před Soudním dvorem Evropské unie, který byl vyvolán společným řízením o předběžné otázce, vznesené irským High Court of Ireland a rakouským Verfassungsgerichtshof[105].

5.4 Nález Ústavního soudu ČR Pl. ÚS 24/10

V České republice se, obdobně jako v jiných členských státech EU, staly hlavním iniciátorem ústavního přezkumu občanská sdružení. Nevládní organizace Iuridicum Remedium[106], která dlouhodobě kritizuje nejen data retention, ale např.

[102] I. Die Grundrechte. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bundestag.de/bundestag/aufgaben/rechtsgrundlagen/grundgesetz/gg_01/245122
[103] Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011
[104] National legal challenges to the Data Retention Directive. [online]. [cit. 2015-03-23]. Dostupné z: http://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
[105] Rozsudek Soudního dvora (velkého senátu) z 8. dubna 2014. [online]. [cit. 2015-03-23]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=CS
[106] Iure. [online]. [cit. 2015-03-24]. Dostupné z: http://www.iure.org/

rovněž nadužívání bezpečnostních kamer, však nedisponovala aktivní legitimací k podání návrhu Ústavnímu soudu na zrušení příslušných ustanovení zákona o elektronických komunikacích. Pro toto podání tak využila skupinu 51 poslanců v čele s Markem Bendou a Kateřinou Jacques, kteří v březnu roku 2010 tento návrh učinili[107]. Bylo to tak již poté, co se v obdobné věci k transponované směrnici kriticky vyjádřily soudy Rumunska, Bulharska, Kypru, ale především Německa (soudy buď národní transpozici zrušily, nebo pozastavily její účinnost). V návrhu, který navrhoval zrušení ustanovení § 97 odst. 3, 4 a související vyhlášky 485/2005 Sb., o uchovávání provozních a lokalizačních údajů stěžovatelé namítali, že se jedná o nepřiměřený zásah do lidských práv a svobod, především do práva na soukromí.

Terčem kritiky se stala, obdobně jako v jiných zemích, skutečnost, že stát přenáší tuto povinnost na soukromé subjekty, čímž roste riziko kompromitace těchto dat a rovněž to, že cíle, které jsou touto úpravou sledovány, jsou v hrubém nepoměru se zásahem do ústavně zaručených práv, konkrétně základních práv garantovaných čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 Listiny základních práv a svobod a čl. 8 Úmluvy o lidských právech. Obecně lze říci, že v návrhu nezazněly jiné argumenty, nežli ty, které již byly použity před soudy jiných zemí. Rovněž nebyl uplatněn návrh na zrušení oprávnění, jakým jsou tato data vyžadována (podrobně rozebráno v kapitole 3.6.). Obdobně jako německý soud pak stěžovatelé navrhovali, aby Ústavní soud zvážil možnost předložit Evropskému soudnímu dvoru (v souladu s čl. 234 Smlouvy o založení ES)[108] předběžnou otázku týkající se (ne)platnosti samotné Směrnice o data retention, která byla, dle jejich názoru, v rozporu s právem ES.

5.4.1 Názor Ústavního soudu

Ústavní soud konstatoval, že podání návrhu na zrušení příslušných ustanovení sice splňovalo formální náležitosti podle čl. 87 odst. 1 písm. a) Ústavy České republiky a § 64 odst. 1 písm. b) zákona č. 182/1993 Sb., o Ústavním soudu, avšak primárně slouží tento nástroj jako ochrana parlamentní menšiny proti zvůli většiny. Parlamentní menšina totiž nedisponuje zákonodárnými mechanismy jak

[107] Marek Benda a spol. ve sněmovně protestovali proti špiclování lidí. [online]. [cit. 2015-03-24]. Dostupné z: http://www.parlamentnilisty.cz/politika/poslanecka-snemovna/Marek-Benda-a-spol-ve-snemovne-protestovali-proti-spiclovani-lidi-161030

[108] Soudní dvůr EU má pravomoc rozhodovat o předběžných otázkách týkajících se platnosti a výkladu aktů přijatých společenstvím a ECB. (Smlouva o založení Evropského společenství. [online]. [cit. 2015-03-24]. Dostupné z: http://www.euroskop.cz/gallery/2/756-smlouva_o_es_nice.pdf)

zvrátit přijetí zákona, který je dle jejich názoru v rozporu s ústavou. Oproti tomu soud konstatoval, že parlamentní většina těmito prostředky disponuje a v případě pochybností o ústavní konformitě má nejen právo, ale dokonce povinnost takový zákon zrušit či upravit. Navrhovatelé pak patří nejen k parlamentní většině, ale rovněž se na přijetí napadaného zákona přímo podílejí. Pokud by v budoucnu mělo docházet k takovému zneužívání Ústavního soudu, byl by soud nucen takovéto návrhy odmítat.

Před vlastním přezkumem pak Ústavní soud zvážil dále návrh poslanců předložit Evropskému soudnímu dvoru předběžnou otázku týkající se rozporu evropské směrnice o data retention s komunitárním právem. Obdobně jako německý soud tento návrh odmítl s poukazem na to, že obsah směrnice ponechává České republice dostatečný prostor pro ústavně konformní transpozici. Dále vymezil soud referenční hlediska pro posouzení návrhu, kterými se stalo právo na respekt k soukromému životu a informačnímu sebeurčení, stejně jako přípustnost zásahu do práva na informační sebeurčení.

V těchto otázkách Ústavní soud konstatoval, že právo na nerušený soukromý život osoby požívá v liberálních státech zcela zvláštní respekt a ochranu. Primární funkcí práva na respekt k soukromému životu je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti, stejně jako garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Tedy, že jednotlivec má právo samostatně rozhodnout podle svého uvážení, jakým způsobem, v jakém rozsahu, a zda vůbec mají být informace z jeho života zpřístupněny jiným subjektům (což je oním právem na informační sebeurčení). Toto právo může být veřejnou mocí omezeno pouze výjimečně, a to jen je-li to v demokratické společnosti nezbytné, nelze-li sledovaného účelu dosáhnout jinak a *„(…) je-li to akceptovatelné z pohledu zákonné existence a dodržení účinných a konkrétních záruk proti libovůli. Esenciální předpoklady spravedlivého procesu totiž vyžadují, aby byl jednotlivec vybaven dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci.“*[109] Za použití vlastní ustálené judikatury pak dále ÚS konstatoval, že tato ochrana se vztahuje *„(…) nejen k vlastnímu obsahu zpráv podávaných telefonem, ale i k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor.“*[110]

[109] Čl. 36 Nálezu.
[110] Čl. 32 Nálezu.

Po vymezení těchto hledisek přistoupil Ústavní soud k vlastnímu přezkumu napadených ustanovení.

a) ÚS konstatoval, že vzhledem k tomu, že česká právní úprava byla přijata ještě v době, kdy byla tato směrnice teprve projednávána, je česká úprava vyjádřená především ve vyhlášce 485/2005 Sb. podstatně širší, nežli samotné požadavky definované ve směrnici[111].

b) ÚS jednoznačně podpořil hypotézu, že uchovávání provozních a lokalizačních údajů je stejně závažným zásahem do soukromí, a tudíž zasluhující stejnou ochranu jako odposlech, neboť *„(…) budou-li (údaje) sledovány po delší časový úsek, lze v jejich kombinaci sestavit detailní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob. (…) Z uvedených údajů lze až s 90% jistotou např. dovodit, s kým, jak často a dokonce v jakých hodinách se daný jednotlivec stýká, kdo jsou jeho nejbližší známí, kamarádi či kolegové z práce, anebo jaké aktivity a v jakých hodinách provozuje.“*[112]

c) Kriticky vymezil vágní charakteristiku orgánů oprávněných k vyžádání těchto údajů, stejně jako to, že z předmětného ustanovení zřetelně nevyplývá, na základě jakých právních předpisů je možné data vyžadovat[113].

d) Není jasně a přesně vymezen účel, za jakým jsou tyto údaje oprávněným subjektům poskytovány, a nelze tak proto posoudit skutečnou potřebnost takové zákonné úpravy. Zatímco Směrnice byla vydána s cílem *„(…) zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů,“*[114] tak česká úprava (obdobně jako v některých jiných státech) nedefinuje, o jaké závažné trestné činy se jedná a neobsahuje ani jiná omezení zabraňující libovůli veřejné moci ve využívání (nadužívání) těchto údajů. Zároveň není v českém právním řádu zakotvena povinnost

[111] Čl. 46 Nálezu.
[112] Čl. 44 Nálezu.
[113] Čl. 46 Nálezu.
[114] Čl. 1 odst. 1 Směrnice 2006/24/ES.

informovat, byť následně, dotčenou osobu o tom, že její data byla orgány činnými v trestním řízení vyžádána[115].

e) Napadená právní úprava nedostatečně, či vůbec nestanovuje jasná pravidla na zabezpečení uchovávaných údajů týkající se přístupu třetích stran. Je nutné stanovit jasná pravidla rovněž pro likvidaci těchto údajů[116].

f) Ústavní soud apeloval na zákonodárce, aby došlo ke změně ustanovení § 88a trestního řádu, který upravuje vyžádání těchto údajů pro účely trestního řízení (bez jakékoliv specifikace závažnosti činu), neboť v daném kontextu nerespektuje ústavně-právní limity. Toto ustanovení však nemohl Ústavní soud sám derogovat, neboť nebylo v návrhu napadeno[117].

5.4.2 Orbiter dictum

Ústavní soud dále ve formě Orbiter dicti konstatoval, že si je vědom prudkého rozvoje informačních a komunikačních technologií, které přináší sofistikovanější formy páchání trestné činnosti, avšak to nebrání vyslovit pochybnosti o tom, zda je plošné a preventivní uchovávání údajů nástrojem nezbytným a přiměřeným. S ohledem na to, že, jak Ústavní soud konstatoval, je až 70% trestné činnosti pácháno za použití tzv. anonymních předplacených SIM karet, je nutné zpochybnit i efektivitu takového nástroje. V této souvislosti odkázal na analýzu Spolkového úřadu vyšetřování SRN ze dne 26. 1. 2011[118], která na základě porovnání statistických údajů o spáchané závažné trestné činnosti na území Německa před a po přijetí zákonné úpravy data retention prokázala, že to nemělo téměř žádný vliv na snížení počtu spáchaných trestných činů, ani na míru objasněnosti.

[115] Čl. 47 Nálezu.
[116] Čl. 51 Nálezu.
[117] Čl. 54 Nálezu.
[118] Untersuchung: Vorratsdatenspeicherung ist ineffektiv (26.01.2011). [online]. [cit. 2015-03-23]. Dostupné z: http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,de

5.4.3 Zhodnocení právní úpravy testem proporcionality

V následující kapitole se pokusím podívat se na některé skutečnosti, na které poukazovaly Ústavní soudy některých členských zemí, testem proporcionality, který je Ústavním soudem využíván v případě kolize subjektivních práv.

a) **Kritérium vhodnosti**, tedy, zda je možné dosáhnout omezením subjektivního práva stanoveného cíle.

   První kritérium napadená právní úprava splňuje pouze s výhradou. Pokud je cílem zajištění dostupnosti provozních a lokalizačních údajů nutných k vyšetřování, odhalování a stíhání závažné trestné činnosti, pak je skutečně národní právní úprava schopna tohoto cíle dosáhnout. Jak však poznamenal Ústavní soud, národní úprava nereflektuje skutečnost, že se má jednat pouze o závažnou trestnou činnost, tedy obdobně jako v případě odposlechů, ale ve skutečnosti k vyžádání těchto údajů postačí, *„(…) je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu (…).“*[119]

b) Kritérium potřebnosti, tedy zda stanoveného cíle může být dosaženo způsobem, který se nedotýká základních práv a svobod.

   Druhé kritérium napadená úprava splňuje opět pouze s výhradou. Se současným stavem technologií neexistuje bohužel jiný vhodnější způsob, jak dosáhnout stanoveného cíle. Samotný „data freezing“, tedy pouhé zajišťování údajů, kdy se soudní příkaz dotýká konkrétních osob a pouze o těchto jsou od okamžiku obdržení rozhodnutí soudu sbírány provozní a lokalizační údaje, není z hlediska odhalování závažné trestné činnosti dostatečný. Rovněž zrušení předplacených karet by zřejmě nepostačovalo k tomu vzdát se plošného uchovávání data retention, byť by pravděpodobně vedlo k podstatnému snížení počtu žádostí o vydání těchto údajů[120].

c) Kritérium proporcionality, tedy v tomto konkrétním případě, porovnání práva na soukromí a informační sebeurčení s veřejným zájmem.

[119] Podle § 88a trestního řádu v tehdejším znění.

[120] Poznámka z praxe: Velká část požadavků na vydání provozních a lokalizačních údajů je realizována pouze proto, že orgány činné v trestním řízení zkoumají vazby mezi podezřelými anonymními subjekty s cílem nalézt osobu se známou totožností. U té je následně ověřováno, kdo je držitelem anonymní karty.

> Třetí kritérium napadená právní úprava nesplňuje. Plošné a nevýběrové shromažďování provozních a lokalizačních údajů o všech uživatelích sítí elektronických komunikací je zjevně podstatně hlubším zásahem do ústavně zaručených práv a svobod, nežli veřejný zájem na ochraně společnosti před závažnou kriminalitou. Tato neproporcionalita je prohloubena rovněž dobou, po kterou jsou data uchovávána, a skutečností, že sběr těchto dat je přenesen na bedra soukromoprávním subjektům, které tak mají v případě zneužití, při absenci kontrolních mechanismů, prakticky obdobný přístup k „soukromí“ obyvatel jako veřejná moc. Přestože objem takto uchovávaných údajů je obrovský, není ani tak zajištěna dostatečná efektivita při odhalování závažné trestné činnosti, kterou by se, při značně extenzivním výkladu, dalo v době vzrůstajících teroristických hrozeb porušení práva na soukromí obhajovat. To ukazují dostupné statistiky (viz Tabulka č. 2) a také to, že k páchání trestné činnosti jsou využívány služby, jejichž data uchovávána nejsou, nebo jsou pro orgány činné v trestním řízení nečitelná, anonymní, či podvržená. Namátkou lze uvést páchání trestné činnosti za využití anonymizační serverové sítě TOR[121].

Jak vyplývá ze všech uvedených argumentů, neměl Ústavní soud jinou možnost, nežli zrušit dnem vyhlášení nálezu ve Sbírce zákonů napadená ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích, stejně jako prováděcí vyhlášku č. 485/2005 Sb. o uchovávání provozních a lokalizačních údajů. Na rozdíl od německého soudu však nepřikázal již uchovávaná data zlikvidovat.

Tabulka č. 2 - Statistika počtu objasněných trestných činů, ze které vyplývá, že zrušení data retention nemělo žádný dopad na objasněnost trestné činnosti.

Rok	Zjištěných TČ	Objasněných TČ	% objasněných TČ
2008	343.799	127.906	37 %
2009	332.829	127.604	38 %
2010	313.387	117.685	38 %
2011	317.177	122.238	39 %

[121] Více o fungování TOR na: TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu. [online]. [cit. 2015-03-23]. Dostupné z: http://www.security-portal.cz/clanky/tor-onion-router-syst%C3%A9m-pro-vysoce-anonymn%C3%AD-%C5%A1ifrovan%C3%BD-p%C5%99%C3%ADstup-k-internetu

2012	304.528	120.168	39 %
2013	325.366	129.181	40 %

(Zdroj: Statistiky kriminality. [online]. [cit. 2015-03-23]. Dostupné z: http://www.mvcr.cz/clanek/statistiky-kriminality.aspx)

5.4.4 Situace po vyhlášení Nálezu Ústavního soudu

Zrušení příslušných ustanovení zákona o elektronických komunikacích, stejně jako zrušení prováděcí vyhlášky, se u veřejnosti setkalo s bouřlivým přijetím. Lidsko-právní organizace tento krok jednoznačně přivítaly[122], avšak to samé nelze říci o orgánech činných v trestním řízení. Ty si v celé věci stěžovaly na fakt, že provozní a lokalizační údaje byly často jedinou stopou, díky které se policii podařilo odhalit závažný trestný čin[123].

Bohužel v tomto klimatu došlo i k velmi vyostřené výměně názorů mezi operátory a policií, neboť krátce poté, co Ústavní soud zrušil příslušnou vyhlášku, došlo v Praze, a nejen v ní, k sérii vyděračských útoků na obchodní řetězec IKEA, kdy v pobočce této společnosti na pražském Zličíně byl dokonce nalezen nástražně výbušný systém. Pachatelé při páchání trestné činnosti využívali velké množství mobilních telefonů a velmi efektivně za sebou „zametali“ stopy[124].

Přestože v tomto případě by nepochybně data z telekomunikačního provozu mohla přispět k odhalení pachatelů, nebyla tato data, s poukazem na nález Ústavního soudu, policii vydána, resp. byla jí vydána pouze data, která měl operátor pro vlastní vyúčtování, neboť jiná, typicky lokalizační, již neměl k dispozici. Operátoři nález Ústavního soudu vesměs přivítali, přestože to pro ně znamenalo zvýšené náklady spojené s přenastavením infrastruktury a datových skladů tak, aby nadále nedocházelo k uchovávání těchto dat nad rámec, který operátor potřebuje pro vyúčtování služeb. Tento princip zůstal zachován, operátoři tedy na příkaz soudu vydali údaje vztahující se k požadovanému číslu, avšak pouze ty, které měli sami k dispozici. Ve výsledku to znamenalo, že výtěžnost těchto informací pro potřeby trestního řízení byla zcela marginální. Brzy po vydání nálezu Pl. ÚS 24/10 však došlo k vydání dalšího nálezu, který by znamenal, pokud by nebyla urychleně

[122] Podrobněji na: ÚS: Slídění v komunikaci občanů je protiústavní. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/content/us-slideni-v-komunikaci-obcanu-je-protiustavni
[123] CHALOUPSKÁ, Markéta a Veronika BERNÁ. Policie: Oslepli jsme, nesmíme lidi sledovat přes mobil. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/content/us-slideni-v-komunikaci-obcanu-je-protiustavni
[124] Síť IKEA terorizoval manažer ovládající čtyři jazyky. [online]. [cit. 2015-03-23]. Dostupné z: http://zpravy.aktualne.cz/zahranici/sit-ikea-terorizoval-manazer-ovladajici-ctyri-jazyky/r~i:article:716886/

přijata ústavně konformní zákonná úprava, že v rámci trestního řízení nebude moci policie požadovat data vůbec žádná.

5.4.5 Nález Pl. ÚS 24/11 ze dne 20. 12. 2011

Ústavnímu soudu byl dne 27. května 2011 doručen návrh Obvodního soudu pro Prahu 6, kdy se navrhovatel, u kterého probíhalo řízení o návrhu Vojenské policie na vydání příkazu ke zjištění informací o telekomunikačním provozu v souladu s ustanovením § 88a trestního řádu, domníval, že o tomto návrhu nemůže rozhodnout z důvodů jeho pravděpodobného rozporu s ústavním pořádkem. Soud byl k podání návrhu aktivně legitimován v souladu s čl. 95 odst. 2 Ústavy České republiky a § 64 odst. 3 zákona o Ústavním soudu. Ústavní soud následně rozhodl o derogaci napadeného ustanovení, kterou však stanovil až k datu 30. září 2012. Tím poskytl zákonodárcům dostatečný prostor k nalezení ústavně konformního řešení. Soud při argumentaci svého rozhodnutí použil argumenty vyslovené již v předchozím nálezu, a k samotnému ustanovení § 88a uvedl: „*Lze shrnout, že ačkoliv § 88a trestního řádu obsahuje úplnou právní úpravu přístupu orgánů činných v trestním řízení k údajům o uskutečněném telekomunikačním provozu, tento přístup výslovně podmiňuje pouze tím, že předmětné údaje umožňuje zjistit výlučně k objasnění skutečností důležitých pro trestní řízení. Zákonodárce do napadeného ustanovení především nijak nepromítl požadavek proporcionality zásahu do základního práva s ohledem na sledovaný účel, neboť přístup k předmětným údajům upravil v podstatě jako běžný prostředek zaopatřování důkazů pro účely trestního řízení, a to dokonce vedeného pro jakýkoliv trestný čin.*“[125]

Považuji za velmi zajímavý odlišný názor soudkyně Ivany Janů zveřejněný v tomto nálezu. Soudkyně Janů konstatovala, že Ústavní soud již v několika předchozích nálezech definoval ústavní meze orgánů činných v trestním řízení při získávání informací z telekomunikačního provozu. Konkrétně se vyjádřila: *„Dle interpretace Ústavního soudu takto závazný není jen výrok nálezu, ale i odůvodnění, resp. ty jeho části, jež obsahují ‚nosné‘ důvody. Zároveň je nutno připomenout, že Ústavní soud se dlouhodobě řídí zásadou priority ústavně konformní interpretace*

[125] Čl. 30 Nálezu. [online]. [cit. 2015-03-23]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=pl-24-11

před derogací."[126] Dle jejího názoru je ustanovení § 88a systematicky zařazeno k ustanovení § 88, které se týká odposlechu a záznamu telekomunikačního provozu a je nutné jej k tomuto ustanovení ústavně-právním způsobem interpretovat. Kritikou tak nešetřila obecné soudy, neboť, dle jejího názoru, je nutné požadavky na vydání údajů ústavně konformním způsobem interpretovat, což ustanovení § 88a umožňuje, avšak ze strany OČTŘ taková vůle chybí. Dále uvedla, že: *„(…) žádoucí kultivace praxe orgánů činných v trestním řízení však vede jen přes změnu jejich náhledu na používání prostředků obsažených v trestním řádu proporcionálně k základním právům a svobodám jednotlivce, nikoliv přes (formální) změnu ustanovení, jehož výklad dosud nebyl respektován. Je totiž zřejmé, že nadměrné užívání postupu dle ustanovení § 88a trestního řádu je založeno na rutinní praxi orgánů činných v trestním řízení, a to bez ohledu na to, co Ústavní soud považuje za platné právo. Nová právní úprava na zmíněné ‚inflaci návrhů' na postup podle § 88a trestního řádu proto, obávám se, mnoho nezmění."*[127] Je třeba říci, že tento názor je poměrně ojedinělý, byť z mého osobního pohledu velmi cenný. Bohužel se však domnívám, že současná rozhodovací praxe orgánů činných v trestním řízení, či dokonce výkladová praxe obecných soudů je často natolik formalistická, že pouhou „změnou myšlení" by se nepodařilo zamýšleného účelu dosáhnout. Závěrem soudkyně Janů, de lege ferenda, akcentovala klíčovou roli státního zástupce v trestním řízení, který může rozhodujícím způsobem přispět k ochraně subjektivních práv jednotlivce při rozhodování soudu.

[126] Odlišné stanovisko soudkyně Ivany Janů uvedené v závěru Nálezu. [online]. [cit. 2015-03-23]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=pl-24-11
[127] Tamtéž.

6 Zákonná úprava data retention po nálezech Ústavního soudu

Oprávněné orgány se po obou nálezech Ústavního soudu ocitly v situaci, kdy bylo nutné urychleně přijmout novou zákonnou úpravu. Nejenom, že operátoři nebyli nadále povinni tyto údaje v rozsahu a délce držet, ale pokud by se nepodařilo přijmout do 30. 9. 2012 novou úpravu ustanovení § 88a trestního řádu, nebyly by orgány činné v trestním řízení oprávněny jakákoliv data vůbec vyžadovat. To bylo paradoxně i v zájmu operátorů, neboť po derogaci příslušných ustanovení zákona došlo ke ztrátě právního titulu dožadovat se finanční náhrady za uchovávání provozních a lokalizačních údajů. To se zdá jako rozpočtově neutrální, ale je třeba si uvědomit, že operátoři nadále tyto náklady měli, byť na základě soudního příkazu vydávali jen data ve výrazně „okleštěné“ podobě. Výsledkem legislativních prací bylo přijetí zákon č. 273/2012 Sb., kterým se změnil zákon č. 127/2005 Sb. Tento zákon vyšel ve Sbírce zákonů 18. července 2012 s datem účinnosti 1. října 2012. Do českého právního řádu byly promítnuty změny uvedené v následující kapitole.

6.1 Orgány činné v trestním řízení

Ustanovení novelizovaného § 88a trestního řádu odstranilo vágní vymezení účelu, pro který je možné tato data vyžadovat a zavedlo tuto možnost jen u taxativně vymezených trestných činů a pro úmyslné trestné činy, pro které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně 3 roky. Zároveň je zdůrazněno, že stanoveného účelu nemůže být dosaženo jinak. Rovněž je posílena úloha státního zástupce, neboť příkaz může vydat na písemný a řádně odůvodněný návrh státního zástupce jen předseda senátu, v přípravném řízení pak soudce. Pokud je známa totožnost uživatele, ke kterému se data vztahují, musí být v žádosti uvedena. Poslední pojistkou je pak povinnost informovat dotčeného uživatele policejním orgánem či státním zástupcem po pravomocném skončení věci, a v řízení před soudem po pravomocném skončení věci o tom, že byla vyžádána data vztahující se k jeho telekomunikačnímu provozu. Dotčená osoba pak může do 6 měsíců podat Nejvyššímu soudu návrh na přezkum zákonnosti takového opatření. Přijatá úprava tak obsahově téměř splynula s oprávněním, které se týká odposlechu a záznamu telekomunikačního provozu. Retenční doba byla zachována v délce 6 měsíců.

Novela zákona o elektronických komunikacích taxativně stanovila další orgány (mimo orgány činné v trestním řízení), které jsou oprávněny vyžadovat informace z telekomunikačního provozu. Zároveň provedla příslušné změny v jednotlivých speciálních zákonech. V současné době jsou oprávněnými orgány Policie České republiky, Bezpečnostní informační služba, Vojenské zpravodajství a Česká národní banka. (Více v kapitole 3.7.)

6.2 Vyhláška 357/2012 Sb.

Současně s novelizovanou zákonnou úpravou bylo nutné vydat rovněž prováděcí vyhlášku, která bude detailně specifikovat, jaká konkrétní data budou uchovávána, jak budou předávána a jakým způsobem budou likvidována. Přípravou vyhlášky bylo zmocněno Ministerstvo průmyslu a obchodu. Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, nabyla účinnosti 1. listopadu 2012. Přestože derogační důvody vyslovené Ústavním soudem byly dobře známy, došlo v průběhu připomínkového řízení k pokusům významným způsobem rozšířit pravomoci oprávněných orgánů v oblasti zaznamenávání internetového provozu. Konkrétně Ministerstvo vnitra navrhovalo, že operátor nebude muset držet informace jen na své straně komunikace „síťový identifikátor zdrojové strany komunikace," tedy přidělenou IP adresu a port, ale rovněž „síťový identifikátor cílové strany komunikace." To by v praxi znamenalo, že operátoři by museli zaznamenávat v podstatě celý internetový provoz zájmového uživatele v rámci jednoho připojení (tzv. datová session), tedy i to, jaké internetové stránky v průběhu svého připojení navštívil. Kromě obrovských nákladů, které by si taková úprava vyžádala, je na místě se domnívat, že by se již nejednalo o pouhé provozní údaje, ale že taková služba by měla spíše charakter odposlechu. Přestože se tato úprava nakonec v platné verzi vyhlášky, po protestech operátorů a vlastně i negativním vyjádření Ministerstva průmyslu a obchodu neobjevila, je zřejmé, že je třeba, i přes nález Ústavního soudu a rozpoutanou celospolečenskou diskusi, být stále na pozoru. Platná vyhláška se nakonec ve svém rozsahu a typu zaznamenávaných údajů od vyhlášky derogované nijak zásadně neliší.

6.3 Shrnutí kapitoly

Uchovávání provozních a lokalizačních údajů prošlo v České republice poměrně bouřlivým vývojem. Česká republika nejprve přijala národní úpravu ještě předtím, nežli byla známa definitivní podoba evropské Směrnice 2006/24/ES, což vedlo k tomu, že povinné subjekty byly nuceny uchovávat větší množství údajů. Jako pozitivní je pro změnu nutné hodnotit fakt, že doba uchovávání byla stanovena na nejkratší možnou dobu 6 měsíců. Dosavadní statistiky, včetně již několikrát citované zprávy Evropské komise[128], ukazují, že více než 80% údajů je pak skutečně vyžadováno ve lhůtě do 6 měsíců, kterou tak lze hodnotit jako zcela dostatečnou. Pozitivum české právní úpravy je pak jednoznačně v povinnosti státu hradit provozovatelům elektronických komunikací veškeré náklady, které byly efektivně vynaloženy ke splnění zákonné povinnosti, a to přesto, že forma dlouhodobého účetního odpisu zakoupených zařízení nezohledňuje hodnotu peněz v čase, ani případnou inflaci. I přesto je tato úprava na evropské poměry velmi pokroková. Diskuse týkající se možného zrušení této povinnosti pak nemají základ v ústavně právním hledisku, ale spíše jen v tom politickém.

Nález Ústavního soudu pak poukázal na neústavnost zákonné úpravy, spočívající ve zjevné neproporcionalitě mezi povinností plošného a nevýběrového uchovávání těchto údajů a právem na soukromí a informační sebeurčení. Zároveň poukázal na nedostatečné a neústavní vymezení podmínek, za jakých mohou orgány činné v trestním řízení data vyžadovat, stejně jako vágní vymezení ostatních oprávněných orgánů. Nová právní úprava pak v zásadě respektuje nálezy učiněné Ústavním soudem, resp. rovněž ústavními soudy ostatních členských zemí EU a aktuálně platnou úpravu[129] je možné považovat za přiměřenou. Z hlediska chápání zásahu do soukromí a následné zákonné úpravy pak můžeme opravdu s povděkem kvitovat fakt, že uchovávání provozních a lokalizačních údajů bylo postaveno na roveň odposlechů, tedy zachycování obsahu komunikace, byť dle názoru mnohých se jedná o zásah ještě závažnější.

Z mého pohledu se tak nadále jeví problematickým pouze institut vyžadování těchto údajů mimo trestní řízení[130], tedy za účelem pátrání po hledané a pohřešované osobě nebo při předcházení a odhalování hrozeb v oblasti

[128] Zpráva Komise Radě a Evropskému parlamentu: Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES). [online]. [cit. 2015-03-23]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52011DC0225&rid=2
[129] Právní stav k únoru 2015.
[130] Podle § 68 zákona č. 273/2008 Sb., o Policii České republiky.

terorismu[131]. V širším smyslu je pak možné zamyslet se vůbec nad smyslem uchovávání dat ve stávající podobě, neboť tato povinnost nedopadá na provozovatele internetových služeb[132], kterých je naprostá většina, stejně jako je možné díky anonymním SIM kartám či využívání služeb typu TOR odhalení identity zločince poměrně snadno ztížit, obejít nebo rovnou znemožnit. Statistiky pak dokazují, že data retention má jen zanedbatelný podíl na zvýšení objasněnosti trestných činů.

[131] Podle § 71 zákona č. 273/2008 Sb., o Policii České republiky.
[132] Zákon č. 480/2004 Sb., o některých službách informační společnosti.

7 Rozhodnutí Soudního dvora EU[133]

Jak již bylo uvedeno v předchozích kapitolách, v návrzích adresovaných ústavním soudům v jednotlivých členských státech zaznával často požadavek na vyslovení předběžné otázky směrem k SDEU, která měla zodpovědět, zda samotná směrnice není v rozporu se samotným právem EU, tedy konkrétně s Úmluvou o lidských právech. Tento návrh byl odmítán s poukazem na skutečnost, že rámec vymezený směrnicí poskytuje dostatečný prostor pro ústavně konformní transpozici. Odvážný krok učinil až irský Vrchní soud v případu Digital Rights Ireland Ltd.[134], který předložil SDEU předběžné otázky týkající se souladu směrnice č. 2006/24/ES s právy na respektování soukromého života[135] a právem na ochranu osobních údajů[136]. Druhým soudem, který se na SDEU obrátil, byl rakouský Verfassungsgerichtshof. Zatímco v prvním případě šlo o spor mezi soukromou společností Digital Rights Ireland Ltd. a ministerstvem komunikací, který se týkal sporu o zpracování telekomunikačních údajů společnosti ze strany irských orgánů, v druhém případě šlo o návrh vlády spolkové země Korutany a 11.128 dalších navrhovatelů, kteří k SDEU podali předběžnou otázku ve věci slučitelnosti zákona provádějícího směrnici 2006/24/ES do rakouského vnitrostátního práva se spolkovým ústavním zákonem (Bundes-Verfassungsgesetz). Soudní dvůr EU obě věci projednával ve společném řízení C-293/12 a C-594/12.

7.1 Stanovisko generálního advokáta

Generální advokát Pedro Cruz Villalón přednesl své stanovisko[137], že směrnice o uchovávání údajů je *„(…) v plném rozsahu neslučitelná s požadavkem stanoveným Listinou základních práv Evropské unie, podle kterého musí být každé omezení výkonu některého ze základních práv stanoveno zákonem.“*[138] Dále konstatoval, že směrnice představuje závažný zásah do základního práva občanů na

[133] Ve společném řízení C-293/12 a C-594/12.
[134] Judgement of Mr. Justice William M. McKechnie delivered on the 5th day of May 2010. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bailii.org/ie/cases/IEHC/2010/H221.html
[135] Podle čl. 8 Evropské úmluvy o lidských právech a čl. 7 Listiny základních práv EU.
[136] Podle čl. 8 Listiny základních práv EU.
[137] OPINION OF ADVOCATE GENERAL CRUZ VILLALÓN delivered on 12 December 2013. [online]. [cit. 2015-03-29]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=145562&doclang=EN
[138] Podle čl. 53 Listiny práv a svobod EU.

respektování soukromého života[139]. Poukázal na to, že využívání těchto údajů může vést k úplnému a přesnému zmapování soukromého života, či dokonce k sestavení věrného obrazu soukromé identity občana a kritizoval skutečnost, že údaje nejsou uchovávány samotnými veřejnými orgány, dokonce ani pod jejich přímou kontrolou, ale jsou pod kontrolou samotných poskytovatelů služeb elektronických komunikací. Směrnice nestanovila povinnost, že tato data musí být uchovávána na území členských států Unie, což v případě jejich přenesení do mimoevropského kyberprostoru významně zvyšuje riziko zneužití.

V otázce proporcionality dospěl Villalón k závěru, že směrnice je s touto zásadou neslučitelná[140]. Dále konstatoval, že bude nutné posoudit hledisko záruky ze strany jednotlivých členských států, neboť směrnice sice stanoví rozsáhlé povinnosti, avšak záruky ponechává na členských státech. Poukázal rovněž na vágní vymezení pojmu závažná kriminalita (serious crime) a relativně málo přísné podmínky přístupu k těmto datům, kdy podmínky by měly být přísné stejně, jako je tomu u práva na prolomení lékařského tajemství. Každý přístup k těmto datům by pak měl být omezen na soudní či jiné nezávislé orgány, nebo by alespoň každá žádost měla podléhat kontrole ze strany soudů[141]. Závěrem navrhl generální advokát pozastavení účinků určení případné neplatnosti této směrnice na dobu, nežli členské státy přijmou opatření určená k nápravě konstatované neplatnosti, přičemž ale tato opatření musí být přijata v přiměřené lhůtě.

7.2 Rozhodnutí SDEU

Soudní dvůr Evropské unie zasedající ve velkém senátu s předsedou V. Skourisem se v podstatě ztotožnil se stanoviskem generálního advokáta. Přestože soud konstatoval (první test proporcionality), že směrnice je vzhledem k rostoucímu vlivu elektronické komunikace způsobilým nástrojem k potírání závažné kriminality (jeden z hlavních cílů směrnice), tak zásah do soukromí a zájem na ochraně osobních údajů musí být, v souladu s konstantní judikaturou, minimalizován. Odůvodnění, proč tomu tak není, soud konkretizoval v bodech 58 a 59 a osobně jej považuji za natolik brilantní, že je ocituji v přesném znění:

[139] Podle čl. 7 a čl. 8 Listiny práv a svobod EU.
[140] Podle čl. 5 odst. 4 Smlouvy o EU: *„Podle zásady proporcionality nepřekročí obsah ani forma činnosti Unie rámec toho, co je nezbytné pro dosažení cílů Smluv.“*
[141] Opinion of Advocate General Cruz Villalón delivered on 12 December 2013. [online]. [cit. 2015-03-23]. Dostupné z: https://edri.org/wp-content/uploads/2013/12/C-293-12-AGOP-1.pdf

„Směrnice 2006/24 se totiž týká globálně všech osob, které využívají služeb elektronických komunikací, aniž se však osoby, jejichž údaje jsou uchovávány, nachází byť nepřímo v situaci, která může vést k trestnímu stíhání. Vztahuje se tedy i na osoby, v jejichž případě neexistuje žádný důvod se domnívat, že by jejich chování mohlo byť nepřímo nebo vzdáleně souviset se závažnou trestnou činností. Kromě toho nestanoví žádnou výjimku, takže se vztahuje i na osoby, jejichž komunikace jsou podle pravidel vnitrostátního práva předmětem profesního tajemství. (…) Uvedená směrnice, jejímž cílem je přispět k boji proti závažné trestné činnosti, dále nevyžaduje žádnou souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti a zejména se neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k předcházení, odhalování nebo stíhání závažných trestných činů.“[142]

V bodě 69 rozsudku konstatoval, že *„s ohledem na veškeré výše uvedené úvahy je třeba mít za to, že unijní zákonodárce překročil přijetím směrnice 2006/24 meze, jež ukládá požadavek na dodržování zásady proporcionality z hlediska článků 7 a 8 a čl. 52 odst. 1 Listiny.“*[143] Rozsudek ze dne 8. 4. 2014 tedy zněl: ***„Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES je neplatná.“***[144] Na rozdíl od návrhu generálního advokáta tak SDEU zrušil přezkoumávanou směrnici okamžitě, a to dokonce ex tunc.

[142] Bod č. 58 a 59 rozsudku.
[143] Bod č. 69 rozsudku.
[144] Rozsudek Soudního dvora (velkého senátu) z 8. dubna 2014. [online]. [cit. 2015-03-23]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd3c3946e5953945049d60c9b761fff090.e34KaxiLc3qMb40Rch0SaxuPbhj0?text=&docid=150642&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=85389

8 Následky zrušení směrnice 2006/24/ES

Zrušení evropské směrnice neznamenalo automaticky zrušení národních úprav v jednotlivých členských zemích. Stejně tak u těch zemí, které přijetí směrnice odmítly, nebo v nich byla ústavními soudy zrušena, nelze zahájit řízení pro porušení smlouvy dle článku 258 – 260 Smlouvy o fungování Evropské unie. Celá situace ohledně evropského zákonného rámce týkající se data retention se tak v podstatě vrací do roku 2002, kdy byla přijata směrnice 2002/58/ES o soukromí a elektronických komunikacích[145]. Tato směrnice (jak již bylo řečeno v kapitole 3.4) umožňuje, avšak nenařizuje členským státům možnost přijmout opatření v zájmu národní bezpečnosti, spočívající, mimo jiné, v uchovávání údajů. To však musí být nezbytné, přiměřené a úměrné[146].

V České republice tedy nadále zůstávají účinné veškeré předpisy týkající se data retention, a to ať již jde o jejich ukládání (zákon o elektronických komunikacích, včetně příslušné vyhlášky), tak i pokud jde o jejich vyžadování v trestním řízení (trestní řád). Iniciativa ke změně současné legislativy dosud nevzešla ani ze zákonodárného sboru, ani dosud nikdo s aktivní legitimací nepodal návrh na přezkum ústavnosti Ústavnímu soudu. Situace v Evropě je pak v tuto chvíli poněkud nepřehledná. Zatímco např. Slovensko, Slovinsko, Rumunsko nebo Rakousko uchovávání dat nevyžaduje, byť k tomu nedošlo přímým působením rozsudku SDEU, tak v Dánsku, či Velké Británii zůstala právní úprava prakticky beze změn. V České republice tak po sérii jednání mezi povinnými a oprávněnými subjekty byla zvolena cesta určité zdrženlivosti, kdy je preferováno přijetí nové právní úpravy na úrovni EU.

[145] Směrnice 2006/24/ES měnila směrnici 2002/58/ES (viz kapitola 3.4).
[146] Čl. 15 směrnice 2002/58/ES.

9 Možnost vyžádání provozních a lokalizačních údajů

Současná zákonná úprava nařizuje orgánům činným v trestním řízení, aby po pravomocném skončení věci informovaly dotčeného účastníka, že jeho provozní a lokalizační data byla vyžádána, a každý tak má možnost dovolat se soudního přezkumu tohoto úkonu. Kromě toho má dnes každý zákazník možnost vyžádat si u svého operátora svůj vlastní výpis těchto informací, a to v rozsahu a podobě, v jakých by tato data byla poskytnuta oprávněným subjektům[147]. Průlomem pro tuto možnost se stalo stanovisko Úřadu pro ochranu osobních údajů, které si vyžádal student Jan Cibulka na základě § 12[148] zákona č. 101/2000 Sb., o ochraně osobních údajů. Úřad konstatoval, že*„(…) samotné poskytnutí informace o uchovávaných provozních a lokalizačních údajích subjektu údajů nemůže nijak ohrozit cíl, pro který jsou tato data zpracovávána, a proto omezení takového práva není nezbytným opatřením.“*[149]

Do této doby operátoři skutečně odmítali tyto údaje koncovým zákazníkům zpřístupnit, neboť byli toho názoru, že tyto údaje spadají mezi osobní údaje zpracovávané v souladu s ustanovením § 3 odst. 6 pís. d)[150] zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Operátor T-Mobile byl prvním operátorem, který začal tato data soukromým osobám poskytovat. Jediným problémem, se kterým se musel vypořádat, byla skutečnost, že řada fyzických osob, fyzických osob podnikatelů, či právnických osob používá více než jednu SIM kartu a není tedy vždy zřejmé, zda se vyžadovaná data vztahují skutečně k oprávněné osobě, tedy držiteli telefonního čísla, o jehož data je žádáno. Ve vydávání dat byl tedy zvolen skutečně velmi restriktivní přístup, kdy data k anonymním předplaceným SIM kartám či účastnickým smlouvám s více telefonními čísly (lhostejno, zda ji uzavřela fyzická, či právnická osoba) nejsou vydávána. Vydávání dat je dále podmíněno osobní návštěvou zájemce v sídle operátora, aby mohla být

[147] ROŽÁNEK, Filip a Kateřina KOZMOVÁ. Mobilní operátor musí poskytnout majiteli účtu veškeré archivované údaje. [online]. [cit. 2015-03-23]. Dostupné z: http://www.rozhlas.cz/zpravy/technika/_zprava/mobilni-operator-musi-poskytnout-majiteli-uctu-veskere-archivovane-udaje--1172199

[148] Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.

[149] Poskytnutí provozních a lokalizačních údajů subjektu udajů. [online]. [cit. 2015-03-23]. Dostupné z: https://www.uoou.cz/poskytnuti-provoznich-a-lokalizacnich-udaju-subjektu-udaju/d-1801/p1=1099

[150] Ustanovení § 5 odst. 1 a § 11 a 12 se nepoužijí pro zpracování osobních údajů nezbytných pro plnění povinností správce stanovených zvláštními zákony pro zajištění předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů.

ověřena jeho totožnost. Od února 2013, kdy tato možnost existuje, ji však využily jen jednotky zákazníků.

10 Je soukromí skutečně ohroženo?

Jak vyplývá z předchozích kapitol, představuje data retention a obecně elektronická komunikace poměrně invazivní zásah do soukromí každého z nás. Bohužel to zdaleka není ohrožení jediné. Snad největším skandálem uplynulých let se stala výpověď bývalého zaměstnance americké agentury NSA, Edwarda Snowdena, který svět informoval o projektu PRISM[151], jež masivně sledoval elektronickou komunikaci uživatelů internetu za údajného přispění největších poskytovatelů služeb na světě, jakými jsou Apple, Google, Microsoft, či Facebook (všechny společnosti podíl na sledování odmítly). Veškeré toto sledování se dělo bez jakéhokoliv dohledu nezávislých orgánů či soudní moci.

V Evropě je pro změnu připravován projekt INDECT[152], který si klade za cíl prostřednictvím kamerových systémů využívání dat z internetu, sociálních sítí, P2P sítí, pomocí vysoce sofistikovaných systémů umělé inteligence „předpovídat" hrozby trestné činnosti či abnormálního chování obyvatel. Podobně jako v případě data retention se cíl zdá být bohulibý a sloužící občanům, nicméně na skutečný výsledek musíme ještě počkat.

Podobně „nevinným" je pak projekt e-call, slibující motoristům při nehodě přivolat pomoc. Tedy, každý automobil bude muset být od určitého data vybaven e-call jednotkou, která v případě nehody vozidla automaticky vyšle tísňovou zprávu na linku 112, včetně odeslání lokalizačních dat, kde se vozidlo nachází[153]. Přestože projekt slibuje, že každá jednotka bude aktivní jen v okamžiku nehody, jak si můžeme být jisti? A jak dlouho toto přesvědčení vydrží, pokud se bezpečnostní situace opět zhorší, tak, jako tomu nepochybně bude po útoku na redakci Charlie Hebdo?

Cílem této kapitoly nebylo čtenáře vyděsit, ale spíše klást zneklidňující otázky nutící k zamyšlení. Neboť doba, kdy soukromí bude cennější, nežli cokoliv jiného se bohužel kvapem blíží.

[151] PRISM (surveillance program). In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-23]. Dostupné z: http://en.wikipedia.org/wiki/PRISM_(surveillance_program)
[152] Indect [online]. [cit. 2015-03-23]. Dostupné z: http://www.indect-project.eu/
[153] O systému eCall. *HeERO* [online]. [cit. 2015-03-23]. Dostupné z: http://www.heero-pilot.eu/view/cs/ecall.html

11 Závěr

Cílem této práce bylo přinést čtenáři ucelený pohled na problematiku data retention a její ústavně-právní limity v evropském kontextu. Provedl jsem srovnání klíčových nálezů Ústavních soudů některých členských zemí a poukázal na velmi nejednotný a roztříštěný přístup samotných členských států EU k této problematice. Stejně tak jsem provedl chronologický přehled vývoje data retention v České republice, a to od poněkud překotné implementace Směrnice, až po klíčový nález PL ÚS 24/10.

Čtenář by měl získat ucelenou představu o mimořádně komplikovaném vztahu mezi veřejnou mocí a ochranou soukromí každého občana. Tato proporcionalita a jistý rovnovážný vztah mezi těmito zájmy jsou navíc v dnešní době mimořádně komplikovány tím, že současné a budoucí technologie umožňují (a ještě více umožňovat budou) vstupovat do soukromí občanů způsobem, který se navenek nebude jevit nijak invazivním, ale spíše společensky prospěšným až bohulibým. Je totiž jisté, že využívání lokalizačních údajů při volání na tísňové linky pomáhá významným způsobem zachraňovat občany v nouzi, stejně tak se ale může změnit v naši noční můru v rukou stalkera.

Převládající názor veřejnosti, spočívající v tvrzení „když nedělám nic špatného, nemám se čeho bát“ je pravým požehnáním pro všechny ty, kteří se neustále snaží rozšiřovat limity své veřejné moci. A také je namnoze těmito osobami argumentačně využíván pro skrytou manipulaci veřejnosti. Je potěšující, že Ústavní soud zaujímá v těchto věcech velmi ustálený názor, o čemž svědčí i jeden z jeho posledních nálezů týkající se sociální sítě Facebook[154] a zdůrazňující, že ani částečně soukromá a dobrovolná povaha sítě Facebook nemůže být ze strany orgánů činných v trestním řízení využívána bez limitů stanovených trestním řádem.

Co se týká současné úpravy data retention, bude nepochybně velmi zajímavé, jakým směrem se bude tato úprava vyvíjet po zrušení předchozí směrnice 2006/24/ES. Je velmi pravděpodobné, že většina členských států rezignuje na vlastní, dnes zcela rozdrobenou právní úpravu, ale bude spoléhat spíše na evropský regulační rámec, který bude následně transponovat. Na jedné straně stojí neustále

[154] Povaha sociální sítě Facebook není jednoznačně soukromá či veřejná a orgány činné v trestním řízení musí při zajišťování dat z této sítě postupovat v souladu s trestním řádem. [online]. [cit. 2015-03-23]. Dostupné z: http://www.usoud.cz/aktualne/?tx_ttnews%5Btt_news%5D=2746&cHash=2a4e443657acf7a2db351b9cac9264f8

se zhoršující globální bezpečnostní situace, na straně druhé pak fakt, že dosavadní využívání těchto dat nijak významně nezlepšuje statistiky objasněnosti trestné činnosti. Navíc lze tento monitoring poměrně snadno obejít, a tak je možné, že následky tohoto opatření budou dopadat spíše na spořádané občany.

Při úvahách de lege ferenda je třeba se zamyslet nad dalším zkrácením doby uchovávání těchto údajů a také nad tím, zda by dále neměla být zúžena množina trestných činů, u kterých je možné tato data vyžádat. Nepochybně bude také nutné opětovně otevřít diskusi, zda k dosažení cíle nepostačuje pouhé zajišťování dat „data freezing“. Samotné plošné uchovávání je pak skutečně poněkud nepřiměřené. Byli bychom stejně benevolentní při plošném uchovávání DNA? Osobně se hodlám této problematice věnovat i v budoucnu, kdy bych rád rozšířil aspekty této práce, ať již o přezkum očekávané právní úpravy, nebo i o hlubší rozbor dalších potenciálních hrozeb schopných narušit naše soukromí, které jsem předestřel v předchozí kapitole. S ohledem na vše shora uvedené se domnívám, že cíle práce jsem naplnil v celém plánovaném rozsahu.

12 Resumé

Cílem práce je zmapovat problematiku uchovávání provozních a lokalizačních údajů z pohledu ústavně zaručeného práva na soukromí. Zároveň si práce klade za cíl komparovat klíčová rozhodnutí některých Ústavních soudů členských zemí EU, díky kterým došlo ke změně pohledu odborné i laické veřejnosti na tuto problematiku.

V první a druhé kapitole vymezuji samotné pojmy odposlechu a uchovávání provozních a lokalizačních údajů a některé zajímavé judikáty, které mají vztah k právu na soukromí.

Třetí kapitola shrnuje vývoj zákonné úpravy uchovávání provozních a lokalizačních údajů v České republice. Tato úprava vychází ze Směrnice Evropského parlamentu a Rady č. 2006/24/ES jejíž implementace se stala povinnou pro všechny členské státy EU. Přesto některé státy odmítly tuto směrnici implementovat s poukazem na její neústavnost. Tato zákonná úprava je v práci rozdělena na povinnost operátorů tato data držet a uchovávat a právo oprávněných orgánů tato data vyžadovat. V současné době je retenční doba v České republice stanovena na 6 měsíců a oprávněnými orgány jsou orgány činné v trestním řízení policie české republiky, BIS, Vojenské zpravodajství a Česká národní banka.

Uchovávání těchto údajů je pro operátory spojeno s náklady na vybudování potřebné infrastruktury a datových skladů, přičemž Česká republika patří k jedněm z mála zemí, kde jsou tyto náklady a to operativní i investiční plně hrazeny státem. Tento princip je popsán v kapitole 4.

V dalších kapitolách jsou komparovány nálezy Ústavních soudů Německa, Rumunska a Bulharska, stejně jako klíčový nález Českého ústavního soudu Pl ÚS 24/10, který zrušil zákonnou úpravu v České republice v celém rozsahu.

Po přijetí nové ústavně konformní úpravy zákonné úpravy došlo k tomu, že Soudní dvůr Evropské unii zrušil směrnici 2006/24/ES v celém rozsahu a to ex tunc, neboť je v rozporu s právem na soukromí. V současné době je tedy přístup evropských zemí zcela roztříštěný. Některé země mají stále platnou původní zákonnou úpravu, jiné ji již zrušily. Česká republika patří mezi země, u kterých je národní úprava stále platná. Je tedy zřejmé, že harmonizační přístup evropských zemí k této problematice si tak v blízké budoucnosti vyžádá nový přístup, respektující právo na soukromí občanů evropských zemí.

13 Summary

The aim of this thesis is to map the issue of retention of traffic and location data in terms of constitutionally guaranteed rights to privacy. At the same time the thesis aims to compare some key decisions of the constitutional courts of EU member states, thanks to which a change of professional and general public point of view on this matter happened.

I am defining the concepts of interception and retention of traffic and location data in the first and second chapter and also some interesting rulings, which are related to the right to privacy.

The third chapter summarizes the legal developments of the retention of traffic and location data in the Czech Republic. This adjustment is based on the Directive of the European Parliament and Council Directive no. 2006/24 / EC, the implementation of which became compulsory for all EU Member States. However, some states refused to implement this Directive with reference to its unconstitutionality. This statutory regulation is in practice divided into operators' obligation to retain and keep such data and a right of legitimate authorities require this data. Currently, the retention time in the Czech Republic is set at six months and the legitimate authorities are Criminal justice Police of the Czech Republic, BIS, Military Intelligence and the Czech National Bank.

Keeping these data is for operators associated with the cost to build the necessary infrastructure and data warehousing, while the Czech Republic belongs to one of the few countries where such costs (operational and even investment ones) are fully financed by the government. This principle is described in Chapter 4.

Judgments of the Constitutional Court of Germany, Romania and Bulgaria are compared in subsequent chapters, as well as key finding of the Czech Constitutional Court Pl US 24/10, which abolished the legal rights of the Czech Republic in its entirety. Following the adoption of new, constitutionally-conforming adjustments to statutory regulation was the fact that the European Court of Justice annulled Directive 2006/24 / EC in its entirety and ex tunc because it is inconsistent with the right to privacy. Currently, the attitude of European countries is completely fragmented. Some countries still have a valid original legal rights, other countries have abolished it. Czech Republic ranks among the countries where the national regulation is still valid. It is therefore obvious that the harmonization approach of European countries to this issue will in the near future require a new approach that respects the right to privacy of citizens of European countries.

14 Zdroje

Publikace

- ČENTÉŠ, Jozef. *Odpočúvanie - procesnoprávne a hmotnoprávne aspekty*. 1. vyd. V Bratislave: C.H. Beck, 2013, xviii, 250 s. Beckova edícia právne inštitúty. ISBN 9788089603091.
- LLOYD, IAN, MELLOR, DAVID P. *Telecommunications law* 1. vyd. Croydon (UK): Sweet & Maxwell, 2013, 261 s. ISBN 978-0-41402-697-1
- MATES, Pavel, Jindřich ŠKODA a František VAVERA. *Veřejné sbory*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2011, xx, 363 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-604-2.
- MATES, Pavel. *Ochrana soukromí ve správním právu.* Praha: Linde, 2004, 307 s. ISBN 8072014587.
- MATES, Pavel. *Nové policejní právo: právní předpisy s komentářem: podle stavu k 1. 1.2009.* Praha: Linde, 2009, 338 s. ISBN 9788072017430.
- SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004, xxx, 770 s. Právo a hospodářství (C.H. Beck). ISBN 80-7179-765-0.
- SVÁK, Ján. Ochrana ľudských práv: (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práv). 2. rozš. vyd. Žilina: Poradca podnikateľa, 2006, s. 425. ISBN 8088931517.
- *Právo na soukromí*. 1. vyd. Editor Vojtěch Šimíček. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011, 212 s. ISBN 9788021054493.
- WAGNEROVÁ, Eliška, *Listina základních práv a svobod: komentář*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012, xxv, 906 s. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-750-6.

Právní předpisy

- Evropské úmluvy o lidských právech.
- Listina práv a svobod EU.
- Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS
- Směrnice Evropského parlamentu a Rady 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. [online]. [cit. 2015-

03-22]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:cs:PDF

- Směrnice Evropského Parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046&from=CS
- Směrnice Evropského Parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/EC.
- Smlouva o Evropské unii.
- Smlouva o založení Evropského společenství. [online]. [cit. 2015-03-24]. Dostupné z: http://www.euroskop.cz/gallery/2/756-smlouva_o_es_nice.pdf
- Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů.
- Ústava Bulharské republiky (dostupná v anglickém jazyce). [online]. [cit. 2015-03-23]. Dostupné z: http://www.parliament.bg/en/const
- Ústava Rumunské republiky (dostupná v anglickém jazyce). [online]. [cit. 2015-03-23]. Dostupné z: http://www.cdep.ro/pls/dic/site.page?id=371
- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.
- Ústavní zákon č. 100/1960 Sb., ze dne 11. července 1960, Ústava Československé socialistické republiky. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1960.html
- Ústavní zákon č. 121/1920 Sb., ze dne 29. února 1920, kterým se uvozuje Ústavní listina Československé republiky [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1920.html
- Ústavní zákon č. 143/1968 Sb., o československé federaci.
- Ústavní zákon č. 150/1948 Sb., Ústavní zákon ze dne 9. května 1948, Ústava Československé republiky [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/docs/texts/constitution_1948.html
- Vyhláška 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech. [online]. [cit. 2015-03-22]. Dostupné z: http://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/rlp/dokumenty/mezinarodni-pakt-o-obcanskych-a-politickych-pravech-a-mezinarodni-pakt-o-hospodarskych--socialnich-a-kulturnich-pravech-19852
- Vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
- Vyhláška č. 462/2013 sb., 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. [online]. [cit.

2015-03-23]. Dostupné z:
http://www.psp.cz/sqw/sbirka.sqw?cz=462&r=2013

- Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.
- Vyhláška č. 486/2005 Sb., kterou se stanoví výše a způsob úhrady efektivně vynaložených nákladů na zřízení a zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby. [online]. [cit. 2015-03-23]. Dostupné z:
http://www.psp.cz/sqw/sbirka.sqw?cz=486&r=2005
- Zákon č. 110/1964 Sb., o telekomunikacích. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=110&r=1964
- Zákon č. 127/2005 Sb., o elektronických komunikacích.
- Zákon č. 140/1960 Sb., trestní zákon, ve znění pozdějších předpisů.
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).
- Zákon č. 151/200 Sb., o telekomunikacích.
- Zákon č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
- Zákon č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, a některé další zákony. [online]. [cit. 2015-03-23]. Dostupné z:
http://www.psp.cz/sqw/sbirka.sqw?cz=265&r=2001
- Zákon č. 273/2008 Sb., o Policii České republiky.
- Zákon č. 273/2012 Sb., zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.
- Zákon č. 40/2009 Sb., trestní zákoník.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti.
- Zákon č. 89/2012 Sb., Občanský zákoník.

Judikatura

- Nález Ústavního soudu ČR Pl. ÚS 24/10.

- Rozhodnutí č. 1258. [online]. [cit. 2015-03-23]. Dostupné z: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf
- Rozhodnutí ve věci Malone proti UK (no. 8691/79) ze dne 2. 8. 1984.
- Rozsudek ESLP ze dne 26. července 2007, Heglas vs. Česká republika, stížnost č. 64209/01.
- Rozsudek ESLP, ze dne 18. dubna 2006, Chadimová vs. Česká republika, stížnost č. 50073/99-
- Rozsudek SDEU ve společné kauze C-293/12 and C-594/12
- Rozsudek Soudního dvora (velkého senátu) z 8. dubna 2014. [online]. [cit. 2015-03-23]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd3c3946e5953945049d60c9b761fff090.e34KaxiLc3qMb40Rch0SaxuPbhj0?text=&docid=150642&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=85389
- Rozsudek Soudního dvora (velkého senátu) z 8. dubna 2014. [online]. [cit. 2015-03-23]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=CS
- Ústavní nález ÚS 502/2000. [online]. [cit. 2015-03-22]. Dostupné z: http://kraken.slv.cz/II.US502/2000
- Ústavní nález ÚS 78/01. [online]. [cit. 2015-03-23]. Dostupné z: http://kraken.slv.cz/IV.US78/01

Elektronické zdroje

- Evaluation report on Data Retention Directive European Commision ze dne 18. 4. 2011. [online]. [cit. 2015-03-22]. Dostupné z: http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf
- ACTA skončila. Europoslanci ji definitivně zamítli drtivou většinou. [online]. [cit. 2015-03-22]. Dostupné z: http://technet.idnes.cz/acta-skoncila-europarlament-zamitl-actu-fdq-/sw_internet.aspx?c=A120704_132333_sw_internet_pka
- BENDA, M. Projev na 36. schůzi poslanecké sněmovny. Poslanecká sněmovna České republiky. [online]. [cit. 2015-03-24]. Dostupné z: http://www.psp.cz/eknih/2010ps/stenprot/036schuz/s036035.htm
- Bulgarian Court Annuls A Vague Article Of The Data Retention Law. [online]. [cit. 2015-03-23]. Dostupné z: http://history.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention
- Český helsinský výbor - historie. [online]. [cit. 2015-03-22]. Dostupné z: http://www.helcom.cz/cs/o-nas/historie/

- Češi uskutečnili 62 milionů silvestrovských hovorů. Zvýšil se i objem dat. [online]. [cit. 2015-03-21]. Dostupné z: http://mobil.idnes.cz/hovory-a-sms-o-silvestru-0xz-/mobilni-operatori.aspx?c=A150101_132220_mobilni-operatori_lhr
- Členové - Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací. [online]. [cit. 2015-03-23]. Dostupné z: http://www.psp.cz/sqw/snem.sqw?id=1139
- Data retention v (nejen) policejní praxi. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf
- DECLARATION ON COMBATING TERRORISM. [online]. [cit. 2015-03-22]. Dostupné z: http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf
- Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions. [online]. [cit. 2015-03-22]. Dostupné z: http://www.statewatch.org/news/2002/aug/05datafd.htm
- Důvodová zpráva k návrhu nové ústavy ČSR. [online]. [cit. 2015-03-22]. Dostupné z: http://psp.cz/eknih/1946uns/tisky/t1227_06.htm
- Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění. [online]. [cit. 2015-03-22]. Dostupné z: http://www.ctu.cz/ctu-online/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.html
- GÜTTLINGER, V. Ústavní soud zrušil část zákona o elektronických komunikacích. Ústavní soud České republiky. [online]. [cit. 2015-03-22]. Dostupné z: http://www.concourt.cz/clanek/5068
- Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES). [online]. [cit. 2015-03-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52011DC0225&rid=2
- HUSTINX, Peter. The moment of truth for the Data Retention Directive. [online]. [cit. 2015-03-22]. Dostupné z: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf
- Hustinx: Data retention is the EU's most invasive tool. [online]. [cit. 2015-03-22]. Dostupné z: http://www.euractiv.com/infosociety/hustinx-data-retention-eus-invas-interview-504243
- CHALOUPSKÁ, Markéta a Veronika BERNÁ. Policie: Oslepli jsme, nesmíme lidi sledovat přes mobil. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/content/us-slideni-v-komunikaci-obcanu-je-protiustavni
- I. Die Grundrechte. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bundestag.de/bundestag/aufgaben/rechtsgrundlagen/grundgesetz/gg_01/245122

- Indect [online]. [cit. 2015-03-23]. Dostupné z: http://www.indect-project.eu/
- Interaktivní mapa BTS. [online]. [cit. 2015-03-22]. Dostupné z: http://www.gsmweb.cz/mapa
- Iure. [online]. [cit. 2015-03-24]. Dostupné z: http://www.iure.org/
- Judgement of Mr. Justice William M. McKechnie delivered on the 5th day of May 2010. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bailii.org/ie/cases/IEHC/2010/H221.html
- Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011
- KMENTA, J.; Syrovátka, T. Policista nelegálně sháněl výpisy mobilů, špehoval i Rychetského. *iDnes.cz*. [online]. [cit. 2015-03-22]. Dostupné z: http://zpravy.idnes.cz/policista-nelegalne-shanel-vypisy-mobilu-spehoval-i-rychetskeho-phy-/krimi.aspx?c=A110617_225431_krimi_abr
- Marek Benda a spol. ve sněmovně protestovali proti špiclování lidí. [online]. [cit. 2015-03-24]. Dostupné z: http://www.parlamentnilisty.cz/politika/poslanecka-snemovna/Marek-Benda-a-spol-ve-snemovne-protestovali-proti-spiclovani-lidi-161030
- National legal challenges to the Data Retention Directive. [online]. [cit. 2015-03-23]. Dostupné z: http://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
- Návrh na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a návrh na zrušení vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. [online]. Dostupné na: http://www.slidilove.cz/sites/default/files/St%C3%AD%C5%BEnost%20k%20%C3%9AS.pdf
- O systému eCall. *HeERO* [online]. [cit. 2015-03-23]. Dostupné z: http://www.heero-pilot.eu/view/cs/ecall.html
- Operátorům nic nedlužíme a nové pravomoce nechceme. [online]. [cit. 2015-03-23]. Dostupné z: http://www.bis.cz/n/2005-03-22-operatorum-nic-nedluzime-a-nove-pravomoce-nechceme.html
- PETERKA, Jiří. Data retention dostalo stopku už i v ČR. [online]. [cit. 2015-03-24]. Dostupné z: http://www.lupa.cz/clanky/data-retention-dostalo-stopku-uz-i-v-r/
- Podrobněji na: ÚS: Slídění v komunikaci občanů je protiústavní. [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/content/us-slideni-v-komunikaci-obcanu-je-protiustavni
- Policista, který šmíroval politické špičky, dostal podmínku. [online]. [cit. 2015-03-23]. Dostupné z: http://tn.nova.cz/clanek/zpravy/domaci/policista-ktery-smiroval-politicke-spicky-dostal-podminku.html

- Poskytnutí provozních a lokalizačních údajů subjektu udajů. [online]. [cit. 2015-03-23]. Dostupné z: https://www.uoou.cz/poskytnuti-provoznich-a-lokalizacnich-udaju-subjektu-udaju/d-1801/p1=1099
- Povaha sociální sítě Facebook není jednoznačně soukromá či veřejná a orgány činné v trestním řízení musí při zajišťování dat z této sítě postupovat v souladu s trestním řádem. [online]. [cit. 2015-03-23]. Dostupné z: http://www.usoud.cz/aktualne/?tx_ttnews%5Btt_news%5D=2746&cHash=2a4e443657acf7a2db351b9cac9264f8
- PRISM (surveillance program). In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-23]. Dostupné z: http://en.wikipedia.org/wiki/PRISM_(surveillance_program)
- Recommendation on the Respect of Privacy in the context of Interception of Telecommunications. [online]. [cit. 2015-03-22]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp18_en.pdf
- ROŽÁNEK, Filip a Kateřina KOZMOVÁ. Mobilní operátor musí poskytnout majiteli účtu veškeré archivované údaje. [online]. [cit. 2015-03-23]. Dostupné z: http://www.rozhlas.cz/zpravy/technika/_zprava/mobilni-operator-musi-poskytnout-majiteli-uctu-veskere-archivovane-udaje--1172199
- Sdělení federálního ministerstva zahraničních věcí č. 169/1991 Sb. [online]. [cit. 2015-03-22]. Dostupné z: http://www.nssoud.cz/zakony/169_1991.pdf
- Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=209&r=1992
- Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících. [online]. [cit. 2015-03-22]. Dostupné z: http://www.psp.cz/sqw/sbirka.sqw?cz=209&r=1992
- Sdělení Ministerstva zahraničních věcí č. 100/2004 Sb.m.s. [online]. [cit. 2015-03-22]. Dostupné z: http://www.gcc.ca/pdf/INT000000019b.pdf
- Síť IKEA terorizoval manažer ovládající čtyři jazyky. [online]. [cit. 2015-03-23]. Dostupné z: http://zpravy.aktualne.cz/zahranici/sit-ikea-terorizoval-manazer-ovladajici-ctyri-jazyky/r~i:article:716886/
- SPD-Zustimmung zur Vorratsdatenspeicherung wäre Betrug am Wähler. [online]. [cit. 2015-03-23]. Dostupné z: http://www.vorratsdatenspeicherung.de/
- Stanovisko generálního advokáta Pedra Cruz Villalóna ze dne 12. 12. 2013 C-293/12 žádost o rozhodnutí podané v předběžné otázce podaná High Court of Ireland a věc C-594/12 žádost o rozhodnutí o předběžné otázce podaná Verfassunsgerichtshof Rakousko. [online]. [cit. 2015-03-23]. Dostupné z: https://edri.org/wp-content/uploads/2013/12/C-293-12-AGOP-1.pdf

- Statistiky kriminality. [online]. [cit. 2015-03-23]. Dostupné z: http://www.mvcr.cz/clanek/statistiky-kriminality.aspx
- Tell-all telephone. [online]. [cit. 2015-03-21]. Dostupné z: http://www.zeit.de/datenschutz/malte-spitz-data-retention.
- Untersuchung: Vorratsdatenspeicherung ist ineffektiv (26.01.2011). [online]. [cit. 2015-03-23]. Dostupné z: http://www.vorratsdatenspeicherung.de/content/view/426/79/lang,de
- Uznesenie Ústavného súdu Slovenskej republiky č. PL ÚS10/2014-29, dostupné z: http://portal.concourt.sk/SearchRozhodnutia/rozhod.do?urlpage=dokument&id_spisu=533863
- Více o fungování TOR na: TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu. [online]. [cit. 2015-03-23]. Dostupné z: http://www.security-portal.cz/clanky/tor-onion-router-syst%C3%A9m-pro-vysoce-anonymn%C3%AD-%C5%A1ifrovan%C3%BD-p%C5%99%C3%ADstup-k-internetu
- VOBOŘIL, Jan. Výhrady o.s. Iuridicum Remedium proti návrhu novely zákona o elektronických komunikacích a některých dalších zákonů upravujících povinnost uchovávat provozní a lokalizační údaje o elektronických komunikacích a způsoby využívání těchto údajů (sněmovní tisk č. 383). [online]. [cit. 2015-03-23]. Dostupné z: http://www.slidilove.cz/sites/default/files/vyhrady_-_senatni_tisk_c._383_-_monitorovani_provoznich_a_lokalizacnich_udaju_o_elektronicke_komunikaci.pdf
- Vote of the General Assembly to Adopt the Universal Declaration of Human Rights (UDHR). [online]. [cit. 2015-03-22]. Dostupné z: http://www.gcc.ca/pdf/INT000000019b.pdf
- Zpráva Komise Radě a Evropskému parlamentu: Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES). [online]. [cit. 2015-03-23]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52011DC0225&rid=2