2006 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 1 PAG. 81–98

PRÁVO NA SOUKROMÍ VERSUS BEZPEČNOST VE SJEDNOCENÉ EVROPĚ: ZAMYŠLENÍ NAD PROBLEMATIKOU „DATA RETENTION".

JAROMÍR HOŘÁK

Soukromí lze definovat jako stav, kdy má osoba možnost komukoli zamezit, aby o ní získával informace, popř. svobodně rozhodovat, komu tyto informace zpřístupní. Informacemi zde rozumíme všechny poznatky a vjemy, a to od možnosti osobu nebo skupinu osob v určitém okamžiku přímo smysly vnímat (pozorovat osoby zrakem, poslouchat, atd.), přes jejich sledování pomocí technických prostředků, až po přístup k rozmanitým záznamům těchto osob či o těchto osobách. Rozsah soukromí člověka lze vymezit negativně: náleží sem vše, co není ze své podstaty veřejné nebo se neděje veřejně. Pojem soukromí úzce souvisí s osobním prostorem, do nějž jednotlivec podle své vůle vpouští jen vybrané osoby. Takovým prostorem je zejména obydlí, ale např. i obsah zavazadel či kapes oděvu. Zvláštní forma soukromí spočívá v jistotě odesílatele, že obsah zásilek a zpráv zůstane utajen až do jejich převzetí adresátem.

Zájem na uchování soukromí má svůj původ ve snaze člověka vyhnout se nebezpečí a chránit sebe a svou skupinu před zásahy vetřelců z vnějšku. Potřeba soukromí se do značné míry překrývá s přirozenou psychickou potřebou jistoty, tedy záruky, že se jak okolní prostředí tak i pravidla, jimiž se toto prostředí řídí nebudou nečekaně měnit a že změny zůstanou pod kontrolou jedince. Nedostatek soukromí a neschopnost podržet si kontrolu nad svým osobním prostorem vede u člověka ke značnému stresu. Takový nedostatek je v rozporu s lidskou důstojností a míra zásahů do soukromí je přímo úměrná zhoršování kvality života člověka. Za zvláštní typ takových zásahů lze považovat ty, které se dějí bez vědomí osob, jejichž soukromí je narušováno. Tyto osoby si sice uchovávají klamný pocit soukromí, jsou však zároveň bez možnosti narušování zamezit a tím jsou vystaveny zvýšenému riziku. Velmi stresující je stav, kdy postižení sice vědí, že jejich soukromí může být narušováno, avšak zároveň nejsou případné narušení s to odhalit ani mu zabránit. Takový stav je charakterizován nejistotou a současně bezmocí a je neslučitelný se svobodou ve filozofickém i právním smyslu.

Z toho, co jsme uvedli, vyplývá, že soukromí a možnost člověka si je uchovat, patří mezi nejdůležitější lidské hodnoty, a tedy v obecném povědomí lidí vysoce ceněné potřeby. To platí i přesto, že míra požadovaného soukromí může být velmi proměnlivá jak v různých historických souvislostech a v různých kulturách, tak i ve vnímání různých

jednotlivců či sociálních skupin. Právo na soukromí lze vnímat jako rámec pro realizaci celé řady dalších práv, včetně práva vlastnického. Z axiologického hlediska (z hlediska teorie hodnot) však lze v lidském soukromí spatřovat účel sám o sobě, který již není třeba pojímat jako prostředek k dosahování jiných účelů. Jako takové patří soukromí k hodnotám, které požívají ochrany práva jako systému pravidel stanovených či uznaných státem a veřejnou mocí vynutitelných. Ochrana soukromí občanů je však zároveň typickým případem kolize různých zájmů a žádoucích cílů, které jak jednotlivci tak lidská společnost jako celek sledují.

V určitých situacích však může být zákonem jednotlivci uloženo podat o svém soukromém životě informaci z důvodů veřejného zájmu, např. vypovídá-li jako svědek. Moderní stát se od svého vzniku neobejde bez rozsáhlého shromažďování mnohdy důvěrných informací o svých občanech pro účely daňové či statistické. Samotná podstata veřejné správy tkví v právu vyžadovat určité údaje, které občané běžně neznámým lidem nesdělují (např. datum narození v dokladech totožnosti u žen). Shromažďování poznatků v podobě nejrůznějších censů a sčítání lidu se od raného novověku stalo jedním z nástrojů, pomocí nichž stát získává určitý přehled o svém obyvatelstvu, jeho počtu, věkové a sociální struktuře a geografickém rozložení, aby tak lépe mohl přizpůsobit svou politiku. V uvedených případech se občan ovšem zříká části svého soukromí vědomě, a to buď z vlastního podnětu nebo na výzvu příslušných orgánů veřejné moci, která zároveň poskytuje záruky, že důvěrné údaje budou použity jen právními předpisy stanoveným způsobem a přístupny jen určenému okruhu úředních osob vázaných povinností uchovat je v tajnosti. Státem sankcionovanou povinností mlčenlivosti jsou typicky vázáni příslušníci určitých profesí či subjekty, které v rámci své činnosti získávají přístup k důvěrným údajům svých klientů.

Odlišná situace nastává ve chvíli, kdy se státní orgány snaží narušit soukromí osob bez jejich vědomí, obvykle za účelem získání informací důležitých pro potlačování zločinnosti či omezení jiných bezpečnostních rizik. Zákony určitého státu mohou takový postup připouštět, jindy k němu dochází bez zmocnění zákonem, či jsou meze tohoto zmocnění překračovány. Legitimní veřejný zájem na odvrácení často velmi závažných útoků proti společnosti, jaké v moderní době představuje politicky motivovaný terorismus, sabotáže, nepřátelská špionáž a zejména aktivity organizovaného zločinu se zde střetává se zájmem na ochraně soukromí každého jednotlivce. Žádný moderní stát se od vzniku tajných policejních složek na počátku 19. století nevzdal možnosti systematicky sledovat vybrané osoby či skupiny osob, podezřelých z páchání zločinů či jinak potenciálně nebezpečných. Avšak ani totalitní režimy 20. století nebyly vzhledem k nízké úrovni technických prostředků schopny zasahovat do soukromí, sledovat a shromažďovat důvěrné údaje prakticky o všech lidech, dokonce i o těch, kteří se vůbec na území daného státu nenacházejí. Teprve nevídaný rozvoj technologií na konci minulého století učinil tuto doposud fantastickou představu velmi blízkou realitě. Na počátku 21. století žijeme v éře *Mass Surveillance*[1], hromadného, plošného sledování občanů orgány státu i soukromými subjekty.

[1] http://en.wikipedia.org/wiki/Mass_surveillance

Právo na soukromí je chráněno ústavou a zákony národních států i úmluvami mezinárodního společenství. **Všeobecná deklarace lidských práv** v článku 12 uvádí, že „nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům." Podobné je znění čl. 17 **Mezinárodního paktu o občanských a politických právech**, přičemž pakt rovněž deklaruje právo každého na zákonnou ochranu proti uvedeným zásahům nebo útokům. Z dokumentů OSN najdeme obdobnou formulaci práva na soukromí i v čl. 16 Úmluvy o ochraně práv dítěte. Zvláštní význam nejen pro státy Rady Evropy má samozřejmě ustanovení **čl. 8 evropské Úmluvy o ochraně lidských práv a základních svobod**. K právu na respektování rodinného a soukromého života se i zde připojuje právo na nedotknutelnost obydlí a korespondence. Na rozdíl od výše uvedených dokumentů OSN Evropská úmluva výslovně přepokládá možnost **kolize** práva na soukromí s jinými veřejnými zájmy. Připouští, že státní orgán může do výkonu tohoto práva zasahovat jen v případech nezbytných v demokratické společnosti a v souladu se zákonem.V odst. 2 čl. 8 úmluva podává i obecný výčet zájmů, jejichž sledování a ochrana může zásahy státních orgánů do soukromí ospravedlnit (důvody ochrany veřejné bezpečnosti, sledování hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrana zdraví nebo morálky nebo ochrana práv a svobod jiných osob). Další úmluvou Rady Evropy, která se týká ochrany soukromí, je např. Úmluva o ochraně práv jednotlivců v souvislosti s automatickým zpracováním osobních údajů z roku 1981.

Se zvláštními ustanoveními věnovanými ochraně soukromí se běžně setkáváme v ústavách a základních zákonech jednotlivých států. I když např. Prohlášení práv člověka a občana nebo původní americký Bill of Rights právo na soukromí výslovně nezmiňuje, přesto je lze řadit mezi ústavní práva tzv. první generace, a to vzhledem k úzké souvislosti s jinak deklarovanou nedotknutelností osoby či obydlí. Tato souvislost je zjevná např. i v případě **čl. 7 a čl. 10 české Listiny základních práv a svobod**. První odstavec čl. 10 zaručuje právo na ochranu osobnosti (lidské důstojnosti, osobní cti, dobré pověsti a jména), zatímco druhý a třetí odstavec chrání před neoprávněným zasahováním do soukromého a rodinného života a před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V čl. 7 odst. 1 se současně deklaruje nedotknutelnost osoby i jejího soukromí. Právo na soukromí se tak řadí mezi nejvýznamnější subjektivní práva, na jejichž ochraně má společnost zvláštní zájem. Na čl. 10 listiny systematicky navazuje čl. 12 o nedotknutelnosti obydlí, jehož odst. 3 lze mimo jiné vnímat jako ochranu před některými typy nezákonných odposlechů.[2] Listina základních práv a svobod je v tomto ustanovení mnohem stručnější, než např. Základní zákon SRN, který v obsáhlém čl. 13 výslovně reguluje použití moderních technologií při sledování občanů bezpečnostními složkami státu. Uvedené ústavní právní normy jsou v národních státech prováděny řadou předpisů z oboru práva občanského, správního i trestního, mezi nimiž specifickou roli zaujímají předpisy na ochranu osobních údajů. V anglosaských zemích se setkáváme s řadou soudních pre-

[2] Srov. Pavlíček, V. a kol.: Ústavní právo a státověda, II. díl, Linde, Praha 2004, str. 82 a násl. a týž autor in: Ústava a ústavní řád České republiky, 2. díl, Linde, Praha 1999, str. 108 a násl.

cedentů postihujících překročení zákonných mezí státními orgány při zásazích do soukromí občanů.

Charta základních práv Evropské unie uvádí v čl. 7 právo na respektování soukromí, a to výslovně včetně ochrany soukromí osobních zpráv či rozhovorů (communications). Následující článek 8 Charty se týká ochrany osobních dat. Z konkrétních směrnic má v tomto ohledu největší význam zřejmě **směrnice 95/46/EC**, o ochraně osobních údajů, která měla harmonizovat předpisy tohoto typu v jednotlivých členských státech. Tato směrnice obsahuje ve svém čl. 2 širokou definici „osobních dat" jako všech informací, vztahujících se k přímo nebo nepřímo identifikovatelné osobě, přičemž je jako příklad uvedena identifikace na základě znaků fyzických, mentálních, ekonomických, kulturních či sociálních. Směrnice obsahuje rovněž ustanovení ohledně přenosu osobních dat ze států EU do států nečlenských, k němuž smí docházet jen tehdy, pokud daný stát poskytuje osobním údajům náležitou ochranu.

Za nejaktuálnější a vysoce důležitou problematiku týkající se zásahů do práva na soukromí lze považovat plošné uchovávání záznamů o telekomunikačním provozu, tzv. **data retention**. Podstatou data retention není zaznamenávání obsahu telefonních hovorů či e-mailových zpráv, ale schraňování tzv. *metadat* – údajů např. o tom, kdo kdy a jak dlouho komu volal telefonem, kdo si s kým vyměňoval zprávy internetové komunikace (e-mail, ICQ, atd.), zprávy SMS, MMS, dále se jedná o záznamy webových stránek navštívených konkrétním uživatelem na internetu. Data retention může rovněž spočívat ve sbírání lokalizačních údajů o mobilních telefonech. Vzniklé databáze umožňují bezpečnostním složkám pomocí tzv. *traffic analýzy* zmapovat sociální síť sledovaných osob a změny jejich chování v čase. Podle představ části odborníků tak lze poměrně snadno vytvořit přehled o aktivitách a vzájemných kontaktech v rámci organizovaných skupin, zabývajících se nezákonnou činností od obchodu s drogami, přes šíření dětské pornografie až po terorismus.

Soukromé subjekty nabízející internetové služby shromažďují data svých klientů zpravidla dva až tři měsíce za účelem vyúčtování telekomunikačních služeb. Kontroversní a mnohdy nezákonné může být vyhodnocování těchto dat soukromými společnostmi, které sledují chování spotřebitelů na internetu za účelem zefektivnění reklamy a marketingu. V souvislosti s politickým vývojem po teroristických útocích islámských fundamentalistů v USA a západní Evropě začalo být zadržování dat částí politických elit a bezpečnostních odborníků vnímáno jako nezbytné opatření v rámci boje proti organizovanému zločinu a terorismu. Vznikl požadavek, aby soukromí provozovatelé telekomunikací měli za povinnost schraňovat data po dobu delší než půl roku a předávat takto vytvořené databáze státním orgánům, které budou moci shromážděná data zpětně analyzovat v rámci vyšetřování i prevence zásadních bezpečnostních rizik. V Evropské unii tyto snahy reprezentuje čerstvě schválená **Směrnice** (návrh 2005/0182(COD))[3] **o uchovávání dat vzniklých v souvislosti se službami veřejné elektronické komunikace** (Directive of the European Parliament and the Council on

[3] http://www.europarl.eu.int

the retention of data processed in connection with the provision of public elektronic communication services and amending the Directive 2002/58/EC).

Od samého počátku však snaha zavést dlouhodobé plošné uchovávání telekomunikačních metadat naráží na odpor významné části politického spektra v členských státech EU a v Evropském parlamentu. Kritici zdůrazňují, že data retention, tak jak je vyžaduje směrnice, je v zásadním rozporu s právem na soukromí občanů, je snadno zneužitelné, drahé a zároveň nemůže dostatečně naplnit slibované cíle zvýšení bezpečnosti.

Přijetí nové směrnice Radou ministrů je vyvrcholením delšího vývoje v evropské bezpečnostní politice, který sice začal ještě před útoky 11. září 2001, byl jimi však výrazně umocněn, stejně jako pozdějšími událostmi v Madridu a Londýně. Významnou roli sehrál i politický tlak ze strany Spojených států amerických. Stojí za zmínku, že ještě koncem 90. let se zdál být trend alespoň v rámci Evropské unie opačný, tzn. ve prospěch maximální ochrany soukromí a osobních dat občanů v rámci elektronické komunikace. V roce 1997 byla přijata Směrnice o ochraně soukromí v telekomunikacích (Telecommunications Privacy Directive **97/66/EC**), navazující na již zmíněnou směrnici o ochraně osobních údajů z roku 1995. Směrnice z roku 1997 do značné míry posílila ochranu soukromí uživatelů telefonů, mobilních telefonů, digitálních televizí a dalších telekomunikačních zařízení, tím že ukládala řadu nových povinností a zákazů provozovatelům těchto služeb. Mimo jiné zaváděla povinnost operátorů mobilních sítí mazat všechna data po uskutečnění hovoru a výrazně omezila možnost soukromých společností užívat data jejich klientů za účelem vlastního marketingu. V podobném duchu byl zpracován i návrh další směrnice, který Evropská komise připravila v roce 2000. Během procesu schvalování však Rada ministrů začala prosazovat, aby do směrnice byla zahrnuta ustanovení týkajících se **povinnosti internetových providerů a telefonních operátorů zadržovat data z telekomunikačního provozu** za účelem jejich užití bezpečnostními službami, policejními a justičními orgány. Návrh byl v červenci 2001 odmítnut Výborem Evropského parlamentu pro občanské svobody (LIBE) s odůvodněním, že by podobná opatření podřídila občany nepřípustné míře všeobecného a velmi intensivního dozoru. Výbor dokonce přirovnal směrnici o data retention k americkému systému sledování Echelon.[4]

Zásadní změna politického klimatu po 11. září 2001 však umožnila Evropské komisi a některým členským státům (Británie, Španělsko) zesílit tlak na Evropský parlament ohledně přijetí směrnice týkající se data retention. Debata na půdě parlamentu trvala řadu měsíců, nakonec však většina evropských poslanců kontroversní návrh schválila. Přes svůj název tato **Směrnice 2002/58/EC „o soukromí a elektronických komunikacích"**[5] zásadním způsobem prolomila ochranu obsaženou v ustanoveních předchozích evropských předpisů. Ve vztahu k směrnici 1995/46/EC tak směrnice z roku 2002 činí ve svém čl. 15 odst. 1, kde uvádí velmi obecně důvody zajištění národní bezpečnosti, z nichž je možno suspendovat ustanovení čl. 5, 6, 8 a 9 předchozí

4 http://www.fas.org/irp/program/process/echelon.htm

5 Delší naglický název zní Directive „concerning the processing of personal data and the protection of privacy in electronic communications sector".

směrnice. Čl. 15 lze vnímat jako generální klauzuli, která členské státy opravňuje, aby za účelem pátrání, vyšetřování a trestního řízení přijaly zákonná opatření k uchovávání dat.[6]

Směrnice rozlišuje v zásadě dva typy dat, k jejichž schraňování může docházet. Tzv. **traffic data** (do češtiny někdy překládáno jako „provozní data") zahrnují veškeré informace o spojeních, ke kterým dochází v telekomunikačních sítích, např. telefonní či telefaxová čísla, e-mailové adresy, čas a délku spojení, formát a objem přenášených dat. Mezi traffic data patří rovněž údaje o technickém charakteru vysílacího zařízení a druhu sítě, v níž ke komunikaci dochází. Druhým typem jsou tzv. **location data** (lokalizační data), která se vztahují na přesné prostorové souřadnice přenosného telekomunikačního zařízení, tzn. na zeměpisnou šířku, délku a vzdálenost od zemského povrchu. Location data představují záznamy o pohybu vysílacího zařízení (typicky mobilního telefonu) v čase. Informace o vysílání pro neomezený okruh příjemců (rádio, televize) nejsou považovány za data ve smyslu směrnice. Výjimku tvoří případy, kdy je vysílání určeno jen pro konkrétního uživatele (internetové videopůjčovny typu video-on-demand a nejspíš i vysílání televize a rádia po internetu či jiné síti, pokud lze z ukládaných dat identifikovat příjemce). Ani v jednom případě ovšem data retention nezahrnuje obsah komunikace.

V následujícím období několik zemí Evropské unie upravilo tuto problematiku ve svých právních řádech. Z členů EU před posledním rozšířením mezi ně patří Spojené království, Irsko, Francie, Belgie, Španělsko, Dánsko a Itálie. Jen v některých z těchto států platí zákony zavádějící povinné uchovávání dat. V Dánsku a Španělsku nebyly zákony o data retention pro odpor veřejnosti vůbec uvedeny v život. Vhodné je se seznámit se situací ve Spojeném království, neboť právě tento členský stát vyvíjel největší úsilí pro zavedení obligatorního schraňování telekomunikačních dat na evropské úrovni. V **Británii** docházelo k zadržování komunikačních dat pro účely jejich využití bezpečnostními orgány státu již od konce roku 2001, kdy takové schraňování umožnil nový protiteroristický zákon (**Anti-Terrorism, Crime and Security Act 2001**). Ve své části 11 tento zákon obsahuje zhruba stejná kritéria pro zadržovaná data jako pozdější evropská směrnice. K zadržování dat však podle tohoto britského zákona dochází jen na bázi dobrovolnosti.

Soukromí provozovatelé telekomunikací uzavírají smlouvy s ministerstvem vnitra, které zároveň upravilo podmínky dobrovolného zadržování dat zvláštní vyhláškou (UK Home Office Voluntary Code of Practice on Data Retention).[7] Tento **Code of Practice** obsahuje oproti části II. protiteroristického zákona či směrnici 2002/58/EC velmi podrobný výčet nejrůznějších typů dat, od telefonních čísel, přes IP adresy počítačů, údaje o připojení ADSL, údaje o založení e-mailových účtů, až po data týkající se zpráv SMS a MMS. Code of Practice věnuje značnou pozornost informacím o chování uživatelů internetu (místo, čas a frekvence připojení na internet či návštěvy e-mailového účtu, návštěvy jednotlivých webových stránek, atd.), neumožňuje však např. zachycovat hesla uživatelů e-mailových schránek či jiná data, jejichž důvěrnost

---

[6] blíže viz http://www.epic.org/privacy/intl/data_retention.html#origins a http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

[7] http://security.homeoffice.gov.uk

se internetový provider zavázal respektovat. Doba, během níž mají být data uložena, se podle Code of Practice pohybuje od 6 do 12 měsíců pro různé typy dat. Přístup k takto získaným údajům má v Británii poměrně široký okruh státních orgánů, od určitých složek policie (National Crime Squad), přes tajné služby (NCIS, SIS), až po celní orgány a centrální finanční úřady. Do jisté míry paradoxně Code of Practice v sekcích 5 a 6 zaručuje, že se získanými daty bude nakládáno v souladu s britskou úpravou ochrany osobních údajů (Data Protection Act 1998) a v mezích zákona o lidských právech (Human Rights Act 1998)[8]. Code rovněž upravuje náhradu nákladů, které telekomunikačním providerům vzniknou při plnění dobrovolně převzatých závazků ke schraňování dat.

Z hlediska pravidel získávání údajů v rámci data retention je v Británii klíčovým předpisem zákon o policejním a obdobném vyšetřování (**Regulation of Investigatory Powers Act 2000 –RIPA**)[9], na nějž výše uvedený Code of Practice odkazuje. Jde o jeden z předpisů, které doplňují britský policejní zákon (Police Act 1997). Zákon RIPA byl od roku 2002 opakovaně měněn právě s ohledem na metody sledování a pátrání. Data retention se týká především část I. hlavy II. ve znění platném od ledna 2004. K důvodům, jimiž RIPA ospravedlňuje užití operativních pátracích prostředků, jež zasahují do soukromí sledovaných osob, patří kromě obvyklé národní bezpečnosti a boje proti zločinnosti i ekonomické zájmy Spojeného království. Vzhledem k sekcím 5 a 6 tohoto zákona je využití dat získaných v rámci data retention vázáno na zvláštní příkaz (warrant), resp. povolení, které na žádost v zákoně taxativně uvedených osob (oprávněných vedoucích pracovníků jednotlivých bezpečnostních složek) vydává ministr vnitra. Sekce 15 a násl. RIPA obsahuje obecné principy pro nakládání s daty, mimo jiné např. povinnost získaná data okamžitě zničit, jakmile jich nebude více potřeba pro účely pátrání a vyšetřování. Právě tato část zákona se stává terčem kritiky pro přílišnou vágnost, neboť např. počet úředních osob, jimž mohou být v konkrétním případě data zpřístupněna či počet kopií, které státní orgány mohou od získaných dat vytvořit jsou omezeny jen „nezbytnou měrou nutnou pro dosažení cíle, k němuž bylo dáno povolení".

Britský zákon ovšem zavádí i praktické kontrolní mechanismy. Vytváří totiž dva samostatné orgány, jejichž úkolem je bdít nad dodržováním pravidel, pokud je bezpečnostními složkami prováděno sledování občanů, včetně vytěžování poznatků na základě data retention. V části IV. v sekci 57 a násl. jsou upraveny pravomoci „Komisaře pro odposlouchávání a sledování komunikací" (**Interception of Communications Commissioner**)[10]. Jedná se o vysokého úředníka jmenovaného přímo britským předsedou vlády, který má za povinnost dozírat na postup ministra vnitra při vydávání již zmíněných povolení ke sledování, kontrolovat, zda je postup bezpečnostních složek v souladu s RIPA a zjišťovat, zda je se zachycenými daty náležitě nakládáno. Za tímto účelem jsou mu jak ministerstvo vnitra, tak i všechny bezpečnostní složky povinny poskytnout vyčerpávající informace a přístup do všech databází. Tytéž povinnosti mají ovšem i soukromé subjekty, které se na základě smlouvy zavázaly ke spolupráci s brit-

[8] http://www.opsi.gov.uk
[9] http://www.opsi.gov.uk
[10] http://www.ipt-uk.com

ským ministerstvem vnitra ohledně data retention. Komisař vykonává pravidelné inspekční návštěvy u zmíněných státních orgánů a zároveň od nich dostává přehledné zprávy o jejich činnosti. Sám komisař pak každoročně předkládá předsedovi britské vlády vlastní souhrnnou zprávu, která je následně odevzdána k nahlédnutí oběma komorám parlamentu.

Ke klíčovým úkolům komisaře patří i spolupráce s dalším kontrolním orgánem, který je ovšem vybaven podstatně většími pravomocemi. Jde o tzv. **Investigatory Powers Tribunal**[11], ustavený na základě sekcí 65 a násl. RIPA. Tribunál má charakter nezávislého justičního orgánu, z části obsazeného soudci z povolání, který projednává stížnosti na činnost bezpečnostních složek výslovně uvedených v příslušných ustanoveních RIPA. Může se na něj obrátit kdokoli, kdo se cítí v důsledku postupu těchto složek poškozen na svých právech, přičemž je výslovně zmíněna i nedotknutelnost soukromí v rámci elektronické komunikace. Příslušné státní orgány i osoby mají za povinnost spolupracovat s tribunálem při jeho vyšetřování obdobně jako s komisařem podle sekce 57 a násl. Tribunál může na základě stížnosti orgánů nařídit zastavení odposlechu, sledování či shromažďování dat, je-li v rozporu s předpisy. Zároveň může tribunál příslušnému orgánu nařídit, aby získaná data zničil, popř. přiznat stěžovateli i finanční náhradu vzniklé škody či újmy.

Podobně jako v Británii, dochází v současné době k rozsáhlému zadržování telekomunikačních dat i v **Irsku**. Ačkoli irská ústava právo na soukromí výslovně nezmiňuje, irský Nejvyšší soud toto právo dovozuje z článků ústavy, které se týkají ochrany osobnosti. V Irsku platí od roku 1988 zákon o ochraně dat (**Data Protection Act 1988**), který mimo jiné pokrýval automatické sbírání a ukládání dat pomocí technických prostředků. Nad dodržováním zákona bdí zvláštní komisař. V 90. letech však Irsko nestačilo rozšířit dosah tohoto zákona v souladu s již zmiňovanou směrnicí 95/46/EC a muselo proto v roce 2000 čelit žalobě Evropské komise. Na přijetí směrnice 2002/58/EC reagoval irský zákonodárný sbor v červenci 2003 rozsáhlou novelou zákona, která umožňovala široký přístup bezpečnostních orgánů k telekomunikačním datům, povinné schraňování dat o telekomunikačním provozu však nezavedl. Vláda si vypomohla podzákonným předpisem (Ministerial Directive), který operátorům mobilních telefonů ukládal schraňovat některá data až po dobu tří let. Na rozdíl od Británie zde od počátku nešlo o dobrovolné smluvní závazky, ale o povinnost všech soukromých subjektů splňujících v předpise uvedená kritéria. Veřejná moc zde ovšem mohla využít skutečnosti, že irské telekomunikační firmy už řadu let před tím dlouhodobě uchovávaly data svých klientů z komerčních důvodů.

Potřebnost takové úpravy irská vláda vysvětlovala nutností implementace směrnice z roku 2002, ač ta obsahuje toliko oprávnění a nikoli povinnost členských států uzákonit data retention. Když se během roku 2004 irská vláda v rámci debaty o zavedení povinného schraňování dat na evropské úrovni postavila na stranu Británie a dalších států prosazujících povinné data retention, snažila se tak zpětně vytvořit závazky odůvodňující existenci domácího předpisu. Po intenzivní diskusi se vládě nakonec po-

[11] http://www.ipt-uk.com

dařilo prosadit povinné zadržování dat jako dodatek k protiteroristickému zákonu (**Criminal Justice Terrorist Offences Act**), který irský parlament schválil v únoru roku 2005. Tento dodatek přejal z předchozích podzákonných předpisů i dobu 36 měsíců, po níž jsou provozovatelé komunikací data povinni uchovávat. Předmětem data retention v Irské republice jsou i nadále především data mobilních telefonů.[12]

Zemí, která brzy a ve značném rozsahu uzákonila povinné zadržování dat poskytovateli telekomunikačních a internetových služeb je **Belgie**. Až do roku 1994 neobsahovala tamní ústava žádné ustanovení poskytující výslovně ochranu soukromí. Belgické soudy však přímo aplikovaly článek 8 Evropské úmluvy. Od roku 1992 platil v Belgii poměrně přísný zákon na ochranu osobních dat, který byl ve druhé polovině 90. let doplněn v souladu se směrnicí 95/46/EC. Zároveň byla zřízena **Komise pro ochranu soukromí** (Commission de la protection de la vie privée), která zprvu podléhala ministerstvu spravedlnosti a posléze byla podřízena parlamentu. Úkolem komise je vyřizovat stížnosti na zásahy do soukromí osob a podávat parlamentu zprávy o aktivitách orgánů veřejné moci i soukromých subjektů, které mohou narušit právo na soukromí.[13]

V roce 1994 byla ústava Belgie doplněna o článek 22, který se svým zněním shoduje s článkem 8 Úmluvy a rovněž zahrnuje výhradu, podle níž lze do práva na soukromí občanů zasahovat jen na základě zákona. Ve stejném roce byl přijat i zvláštní **zákon o ochraně soukromí v komunikacích** (Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées).[14] V původním znění tento zákon upravoval především pravidla pro policejní odposlechy. Od roku 1998 však zákon ukládá telekomunikačním firmám zaznamenávat a ukládat data o provedených telefonních hovorech spolu s údaji, jež identifikují volajícího a volaného. Minimální doba povinného uložení dat pro účely policejního vyšetřování je v zákoně stanovena na 12 měsíců, zatímco určení celkové přípustné délky uložení dat je přenecháno podzákonné úpravě. K vydání vládního dekretu („Arrêté royal"), který by stanovil limity pro zadržování dat telefonními společnostmi, však nedošlo až do roku 2003. Mezitím se ustálila praxe prosazovaná policejními orgány, podle níž jsou údaje o telefonních hovorech ničeny až po uplynutí tří let.

Koncem 90. let uzavřela belgická Federální policie v souvislosti s vyšetřováním pedofilních skandálů dohodu s poskytovateli internetových služeb. Ti mají za povinnost upozornit speciální policejní odbor, kdykoli se na jejich serverech objeví závadný obsah, u nějž je podezření na dětskou pornografii. Následně schválil belgický parlament **zákon o počítačové kriminalitě** (Loi du 28 novembre 2000 relative à la criminalité informatique), který internetovým společnostem přikazuje schraňovat data o chování uživatelů na internetu po dobu nejméně jednoho roku. Maximální doba uložení dat stanovena opět nebyla, přičemž policie prosazovala ukládání v rozmezí tří až pěti let. Zákon rovněž vyžaduje spolupráci internetových firem při dešifrování obsahu,

[12] http://www.privacyinternational.org
[13] http://www.privacyinternational.org
[14] http://www.privacyinternational.org

který byl kódován. Nesplnění povinností ze strany providera může být postihováno správní i trestní sankcí. Zákon o počítačové kriminalitě byl o rok později doplněn dalším předpisem, který zakazuje užívání anonymních internetových připojení, což znamená, že nadále budou společnosti nabízející internetové připojení odpovídat za to, že lze identifikovat každého uživatele v jejich síti.[15]

Na rozdíl od Belgie a Británie došlo ve **Francii** k zavedení povinného schraňování telekomunikačních dat teprve nedávno, v návaznosti na směrnici 2002/58/EC. Ve Francii je nejdůležitějším předpisem upravujícím problematiku data retention pro účely boje s terorismem a organizovaným zločinem bezpečnostní zákon z roku 2003 (**Loi sur la Sécurité Quotidienne, LSQ**). Prosazením tohoto zákona, který nařizuje poskytovatelům internetových služeb uchovávat metadata identifikující uživatele i jejich chování na síti, využila tehdejší francouzská vláda zmocnění v čl. 15 evropské směrnice. Zákon narazil od počátku na značný odpor veřejnosti a nevládních organizací a doposud nedochází k jeho praktickému uplatňování, neboť k němu dosud nebyl vydán prováděcí předpis.

Na podzim roku 2005 se francouzskému ministru vnitra podařilo získat většinu poslanců Národního shromáždění i Senátu pro návrh nového **protiteroristického zákona**. Návrh mimo jiné ukládá četné povinnosti provozovatelům internetových kaváren, kteří musejí napříště uchovávat a na požádání předávat bezpečnostním orgánům provozní data, volaná čísla a IP-adresy, pokud vznikne podezření ohledně teroristických aktivit. Podobně jako operátoři mobilních sítí, i internetové kavárny a jiná veřejně přístupná místa s připojením na internet mají mít podle nového zákona za povinnost schraňovat po dobu minimálně jednoho roku data o spojeních uskutečňovaných jejich zákazníky. Po schválení zákona se skupina levicových senátorů obrátila na francouzskou Ústavní radu se žádostí o přezkum.

Ještě podstatně širší zásahy do soukromí občanů než ve Francii umožňují nejnovější **italské předpisy**. Po bombových útocích v Londýně vydala italská vláda koncem července 2005 zvláštní nařízení, jehož obsah byl posléze parlamentem vtělen do nového zákona. Telekomunikačním společnostem tento zákon ukládá schraňovat data týkající se telefonních hovorů z pevným linek i mobilů prozatím do konce roku 2007. V případě internetu se povinné data retention v Itálii vztahuje jen na provozní data, která musí zůstat bezpečnostním orgánům k dispozici nejméně po dobu šesti měsíců. Nový zákon dočasně (do 31. 12. 2007) suspenduje účinnost předchozích zákonů o ochraně osobních dat, pokud je s nimi požadavek na uchovávání dat v rozporu. Zároveň obsahuje ještě náročnější požadavky vůči internetovým kavárnám, než o kterých se jedná ve Francii. Internetové kavárny se do budoucna musejí ucházet o zvláštní licenci ministerstva vnitra a být vybaveny technickým zařízením umožňujícím zpětně identifikovat konkrétního uživatele. V praxi to znamená, že veřejně přístupné počítače s připojením na internet budou od uživatelů vyžadovat čísla osobního či řidičského průkazu. Pokud bude nový zákon důsledně uváděn do praxe, rozloučí se Italové s anonymitou, kterou dosud mohly poskytovat mobilní telefony. Pro příště by prodejci

[15] http://www.privacyinternational.org

SIM-karet totiž měli od svých zákazníků vyžadovat osobní údaje, jimiž se po zapojení telefonu uživatel v síti bude identifikovat.[16]

Vývoj ve Francii a Itálii probíhal souběžně s jednáním o nové evropské směrnici o povinném uchovávání dat o komunikaci osob, schválené Evropským parlamentem na konci roku 2005. Projednávaná směrnice měla vliv i na příslušná ustanovení nového **zákona o elektronických komunikacích (zákon č. 127/2005 Sb.)**, přijatého v **České republice** na začátku loňského roku. Zákon účinný od 1. května 2005 uvádí český právní řád do souladu s evropskými směrnicemi regulujícími podnikání v oblasti elektronických komunikací a zcela nahrazuje předchozí předpis (zákon č. 151/2000 Sb., o telekomunikacích). Ust. § 97 zákona obsahuje pravidla pro odposlechy a uchovávání provozních a lokalizačních údajů. V odstavci 3 je stanovena povinnost právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uvedené údaje uchovávat a na požádání je poskytnout oprávněným orgánům.

Provozní a lokalizační údaje, na něž se povinné ukládání vztahuje jsou velmi obecně definovány v § 90 a 91 zákona. Provozními údaji (traffic data) se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování. Lokalizačními údaji jsou definovány jako údaje určující zeměpisnou polohu koncového zařízení uživatele. Pro podrobnější úpravu zákon odkazuje na prováděcí předpisy. Ve srovnání s jinými státy Evropské unie, které dosud zavedly povinné ukládání dat, je český zákon přísnější v tom smyslu, že výslovně stanoví maximální dobu po níž mohou být údaje schraňovány, a to na 12 měsíců. Na místě je zmínit rovněž ust. § 97 odst. 6 cit. zákona, které přiznává poskytovatelům komunikací nárok na úhradu efektivně vynaložených nákladů v souvislosti s plněním povinností uvedených v citovaném ustanovení. Formulace je však ve vztahu k data retention nejasná, uvádí-li se, že náhrada poskytovatelům náleží od subjektu, který si „úkon vyžádal nebo uložil".

Počátkem prosince 2005 vydalo Ministerstvo informatiky po dohodě s Ministerstvem vnitra k zákonu o elektronických komunikacích prováděcí **vyhlášku č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání**. Ustanovení § 2 této vyhlášky obsahuje výčet dat, který mají za povinnost schraňovat provozovatelé pevných telefonních linek (odst. 2), veřejných mobilních sítí (odst. 3) a poskytovatelé internetových služeb (odst. 4). U elektronických komunikací s pevným připojením se uchovávají mj. údaje o uskutečněné komunikaci s uvedením typu komunikace, telefonního čísla volaného i volajícího účastníka, datum, čas a délka komunikace. Stranou nejsou ponechány ani veřejné telefonní budky, u nichž bude docházet alespoň k ukládání identifikátorů telefonních karet. U hovorů z mobilního telefonu se krom jiného má zaznamenávat čas a datum dobití kreditu pomocí kupónu a číslo tohoto kupónu ve vztahu k telefonnímu číslu. U služeb sítě Internet se v České republice data retention napříště vztahuje na identifikátory uživatelského účtu, datum a čas zahájení

[16] http://en.wikipedia.org/wiki/Data_retention#Data_retention_in_Italy

a ukončení připojení, IP-adresy, čísla portu a množství přenesených dat v obou směrech. Dále se uchovávání samozřejmě týká podrobných údajů ohledně e-mailových účtů, včetně informací o použití zabezpečené komunikace. Údaje se (na rozdíl od úpravy zákona č. 127/2005 Sb.) podle § 4 vyhlášky schraňují po dobu minimálně 6 měsíců, v některých případech jen po dobu 3 měsíců. Provozovatel telekomunikace i orgán oprávněný k vyžádání dat mají dle vyhlášky vytvořit kontaktní pracoviště, která budou předávání údajů zajišťovat, přičemž komunikace mezi těmito pracovišti má přednostně probíhat v elektronické formě, způsobem předávání datových souborů.

Prováděcí vyhláška Ministerstva informatiky je zcela v intencích nejnovější **Směrnice** (návrh 2005/0182 (COD) **o uchovávání dat vzniklých v souvislosti se službami veřejné elektronické komunikace.**[17] Tato směrnice má sjednotit postup členských států ohledně data retention a to ve smyslu všeobecné povinnosti provozovatelů telekomunikačních služeb údaje uchovávat. Velkou roli při přijetí směrnice sehrál politický tlak, který Británie vyvinula během svého předsednictví Evropské unii. Vláda Británie obratně využívala psychologického dopadu, který na evropskou veřejnost i politickou reprezentaci měly teroristické útoky v Londýně v červenci roku 2005.

Již záhy po útocích v Madridu na jaře 2004 přijala Evropská rada jako vrcholný politický orgán EU Deklaraci o boji s terorismem, která obsahovala též výzvu Radě EU, aby zkoumala možnost zavedení povinného schraňování telekomunikačních dat v celé unii. Následně podnítily Británie, Francie, Irsko a Švédsko návrh na vydání Rámcového rozhodnutí o uchovávání dat (Council Framework Decision on Data Retention). O návrhu probíhaly od srpna 2004 konzultace Evropské komise a záhy vyvstaly pochybnosti, zda může být předpis takového charakteru přijat v rámci Třetího pilíře (viz část IV. Smlouvy o založení EU, týkající se justiční a bezpečnostní spolupráce). Objevila se pochopitelně i argumentace rozporem návrhu rámcového rozhodnutí s čl. 8 Úmluvy, s čl. 7 Charty základních práv EU a s výše zmíněnými evropskými směrnicemi o ochraně osobních údajů. V prvních měsících roku 2005 museli zastánci návrhu rámcového rozhodnutí čelit ostré kritice ze strany nevládních organizací i sdružení poskytovatelů telekomunikačních služeb. Návrh rámcového rozhodnutí počítal s minimální dobou uložení dat v délce jednoho roku, popř. 6 měsíců pro státy, které by si vymohly výjimku, jež by ovšem musela být každoročně přezkoumávána. V samotné Radě EU docházelo k neshodám mezi delegáty jednotlivých zemí ohledně rozsahu dat, na něž se rámcové rozhodnutí mělo vztahovat. Zpočátku patřilo k hlavním odpůrcům data retention Německo, jehož Spolkový sněm nařídil ministru vnitra nepřistoupit na žádnou povinnost zadržování telekomunikačních dat pro německé společnosti.[18]

V květnu 2005 byl návrh odmítnut Výborem pro občanské svobody Evropského parlamentu (LIBE). Zpráva výboru zdůrazňovala nezvládnutelné množství dat, které by při povinném uchovávání nutně muselo vznikat a v němž by za čas bylo velmi obtížné a nákladné nalézt konkrétní údaj. Průměrné náklady, které by musela ročně vynaložit větší telekomunikační společnost, by se tak pohybovaly kolem 180 milionů

[17] http://www.iure.org/559561
[18] http://www.iure.org/539450

eur.[19] Výbor nejen že vyjádřil pochybnost o souladu návrhu rámcového rozhodnutí s principem proporcionality a s čl. 8 Úmluvy, popř. čl. 7 a 8 Charty, ale odmítl tento návrh i z důvodu rozporu návrhu se směrnicí 2002/58/EC s odkazem na čl. 47 Smlouvy o EU.[20] Skutečnost, že matérie data retention spadá vzhledem k jejím předpokládaným dopadům na společný trh v oblasti telekomunikací alespoň zčásti do **působnosti komunitárního práva (I. pilíř EU)** a musí být tudíž upravena směrnicí a nikoli rámcovým rozhodnutím musela záhy ve svých analýzách uznat i právní oddělení Rady i Komise. Znamenalo to jednak, že návrh měl správně vzejít od Evropské komise a nikoli od členských států, jak se dělo dosud v rámci III. pilíře EU. Především tak do hry podstatně výrazněji vstoupil Evropský parlament, jenž má ohledně směrnic stejnou rozhodovací pravomoc jako Rada. Radě však postačí schválit směrnici kvalifikovanou většinou a nikoli jednomyslně jako u rámcových rozhodnutí.

Takový vývoj by byl další jednání o kontroverzní úpravu pravděpodobně pohřbil, nebo přinejmenším značně pozdržel. Teroristické útoky v Londýně však opět změnily politické klima. Británii se během jejího předsednictví EU podařilo o nutnosti přijetí nové směrnice přesvědčit nejprve Evropskou komisi a posléze prosadit schválení směrnice i v Evropském parlamentu, kde k tomu došlo na základě dohody dvou největších frakcí (EPP-ED a PSE)[21]. Směrnice byla nakonec schválena v rekordním čase (14. prosince 2005, za pouhé tři měsíce po předložení návrhu), a to v prvním čtení 378 hlasy proti 197, aniž byly přijaty pozměňovací návrhy umožňující trvalé výjimky pro ty členské státy, jejichž politické reprezentace i veřejnost uchovávání telekomunikačních dat odmítají. Kritici, mezi kterými byl i parlamentní zpravodaj k návrhu Alexander Alvaro, poukazovali na neúplnou diskusi, která přijetí směrnice předcházela. Rada (ve složení ministrů vnitra a spravedlnosti) směrnici schválila na konci února letošního roku.[22]

Shrnutí **argumentace ve prospěch** obligatorního sběru a ukládání dat nalezneme v memorandu, kterým se uvádí původní návrh Komise předložený v září 2005. V prvních odstavcích se zmiňuje rostoucí význam provozních a lokalizačních dat pro vyšetřování organizované kriminality a pro boj proti terorismu. Prohlášení popisuje, jakým způsobem mohou uchovávaná metadata pomoci při dopadení pachatelů (tedy nikoli při prevenci) závažné trestné činnosti. Vzhledem k tomu, že vyšetřování komplikovaných případů organizovaného zločinu často trvá delší dobu, je potřeba, aby policejní složky měly data o telekomunikačním provozu k dispozici i s odstupem několika let. Provozovatelé telekomunikací však v poslední době vzhledem k novému vývoji technologií údajně zkracují období, po něž jsou metadata uchovávána za účelem vyúčtování nebo z jiných komerčních důvodů. Memorandum dále zmiňuje legislativu jednotlivých členských států, které již povinné zadržování dat zavedly, z čehož vyvozuje potřebu harmonizace. Nová směrnice má navázat na starší evropské předpisy o ochraně osob-

[19] K odhadovaným nákladům blíže srov. http://www.edri.org/edrigram/number4.1/dataretentioncosts
[20] http://www.privacyinternational.org
[21] http://www.linuxzone.cz
[22] blíže k projednávání směrnice viz http://www.edri.org/edrigram/number4.4/dataretention

ních údajů a telekomunikacích, zejména doplnit směrnici 2002/58/EC. Ohledně možného rozporu s čl. 7 a 8 Charty základních práv EU memorandum odkazuje na čl. 52 odst. 1 téhož dokumentu, který umožňuje práva garantovaná chartou omezit pokud je to nutné pro dosažení obecně uznávaných cílů, za účelem ochrany práv a svobod a v souladu s principem proporcionality. Za všeobecně uznávaný cíl prohlašuje komise boj se zločinem a terorismem. Komise zdůrazňuje, že sběr dat se netýká obsahu komunikace, který má podléhat i nadále zcela odlišnému režimu a odkazuje na záruky ochrany osobních údajů obsažené ve směrnicích 95/46/EC a 2002/58/EC.

Podle Komise vychází záměr směrnice plně z **principu subsidiarity**. Cílem směrnice je usnadnit spolupráci bezpečnostních složek a harmonizovat předpisy o data retention tak, aby uchovávané údaje byly ve všech státech k dispozici za obdobných podmínek. Tohoto cíle může být dosaženo nejlépe legislativním zásahem EU, zatímco samostatný postup jednotlivých členských států by nebyl zřejmě účinný. Dále je vysloven předpoklad, že sladění pravidel pro data retention v celé unii ulehčí situaci samotným provozovatelům komunikací, kteří budou moci snáze sjednotit své technologické postupy při schraňování dat, což tyto postupy zlevní. Princip **proporcionality** je dle názoru Komise rovněž zachován, neboť dopady směrnice na soukromí občanů i na zájmy dotčených právnických osob jsou ty nejmenší, při nichž lze ještě dosáhnout sledovaného cíle. V memorandu se tvrdí, že směrnice usiluje o rovnováhu mezi zájmem na ochraně soukromí jednotlivců a nutností hájit právo na život (ohrožované terorismem, zločinem, atd.) jako základní lidské právo. Členské státy budou mít za povinnost upravit svůj právní řád tak, aby byla získaná data dostupná jen na základě zákona a zákonem určeným subjektům za současného respektování práv zaručených Úmluvou. Celkově autoři návrhu vidí směrnici jako kompromis mezi nároky bezpečnostních orgánů, zájmy soukromých společností provozujících telekomunikační služby a argumenty nevládních organizací a subjektů zabývajících se ochranou lidských práv.

Vlastní směrnice je poměrně stručná. Čl. 1 odst. 1 shrnuje cíle směrnice (harmonizace a jistota, že data budou k dispozici pro vyšetřování, odhalování a stíhání organizovaného zločinu a terorismu), čl. 1 odst. 2 uvádí rozsah uchovávaných dat („traffic data", „location data" a údaje umožňující identifikovat uživatele). Výslovně se stanoví, že se zadržování dat nemá týkat obsahu komunikace. Následující čl. 2 obsahuje definice klíčových pojmů a odkazuje na pojmosloví směrnic 95/46/EC a 2002/58/EC. Čl. 3 ukládá členským státům vlastní povinnost přijmout taková zákonná opatření, aby bylo zajištěno uchovávání dat v určeném rozsahu, přičemž tato data musí být k dispozici příslušným orgánům v souladu s právní úpravou členského státu a za účelem stanoveným směrnicí. Data musí být uchovávána takovým způsobem, aby jich bylo možno na požádání příslušných orgánů využít pro účely vyšetřování, pátrání či trestního stíhání (čl. 8). Během projednávání se nepodařilo prosadit pozměňovací návrh, podle nějž by nedocházelo k ukládání údajů o nepřijatých telefonních hovorech, takže i tato data mají být zahrnuta. Odst. 2 ovšem rozlišuje mezi daty o nepřijatých hovorech (unsuccessful call attempts, srov. i čl. 2 odst. 2 písm. f) směrnice), která se zadržují a daty v případech, kdy vůbec nebylo možné spojení navázat (unconnected calls), na

něž se směrnice nevztahuje. Čl. 4 odkazuje ohledně pravidel pro vyžádání dat za účelem vyšetřování na právní úpravu jednotlivých členských států, přičemž tato úprava má odpovídat zásadám proporcionality a být v souladu s právem EU a Úmluvou, tak jak ji vykládá Evropský soud pro lidská práva.

Obsáhlý čl. 5 obsahuje kategorie schraňovaných dat Má se už tradičně jednat o údaje sloužící k identifikaci zdroje i příjemce, k zjištění času, trvání a typu komunikace. Sbírat se budou i data charakterizující technický přístroj, jehož prostřednictvím ke komunikaci dochází a stranou nezůstanou samozřejmě ani data lokalizační. Původní návrh směrnice pro technické podrobnosti odkazoval na zvláštní dodatek, který měl být pravidelně aktualizován. Nyní je většina technických podrobností zařazena přímo do ustanovení čl. 5. Původní návrh komise neznal maximální délku uchovávání údajů a ponechával její určení na legislativě členských států. Minimální délka uchovávání dat měla být původně stanovena na šest měsíců u komunikace užívající výhradně Internet Protocol a v ostatních případech na jeden rok od okamžiku komunikace. V konečném znění směrnice stanoví čl. 6 obecnou minimální dobu pro data retention na **6 měsíců** od okamžiku komunikace. Maximální doba uchovávání byla stanovena na **dva roky**. Čl. 12 však umožňuje členským státům „za zvláštních okolností" tuto hranici překročit. Má však za povinnost o tom neprodleně zpravit Komisi, která během šesti měsíců rozhodne a o přípustnosti takového opatření. Za zmínku stojí, že jediným kritériem, uvedeným v čl. 12 odst. 2 je slučitelnost s pravidly společného trhu. Pokud Komise rozhodne o přípustnosti prodloužení uchovávání dat v určitém členském státě, může tuto výjimku navrhnout jako dodatek ke směrnici. Naopak čl. 15 odst. 3 dává členským státům právo odložit aplikaci směrnice ohledně některých typů dat (data týkající se přístupu na internet, e-mailových účtů a internetových volání) až do uplynutí tří let od schválení směrnice.

Podle čl. 15 mají členské státy směrnici do svých právních řádů transponovat do 18 měsíců od jejího přijetí. Co se týče finančních nákladů na data retention, jsou za jejich uhrazení soukromým subjektům odpovědné členské státy. Směrnice v tomto ohledu nic bližšího nestanoví. Evropská komise bude od členských států dále vyžadovat každoroční statistiky (čl. 10), jež mají poskytovat přehled o případech, kdy si příslušné orgány vyžádaly uchovávaná data, a to včetně doby, která uplynula od okamžiku komunikace do vyžádání. Statistiky budou zahrnovat i případy, kdy žádosti o poskytnutí dat nemohlo být vyhověno. Na jejich základě podá Komise do tří let vyhodnocení Evropskému parlamentu.

Oproti původnímu návrhu obsahuje konečné znění směrnice více **ustanovení týkajících se zabezpečení sbíraných dat proti zneužití**. Směrnice jednak opakovaně odkazuje na zásady ochrany osobních údajů obsažené ve starších směrnicích. Čl. 7 písm. b) a c) zavazuje členské státy k opatřením, která mají zabránit náhodnému nebo protiprávnímu zničení uchovávaných dat, jejich ztrátě, změnám a nezákonnému nakládání vůbec. Písm. d) cit. ust. nařizuje zničení dat po uplynutí zákonné doby jejich uchovávání. Členské státy jsou dále zavázány postihovat zneužití schraňovaných dat trestními i jinými sankcemi (čl. 13 odst. 2). Každý stát má navíc určit nezávislý orgán, který bude nakládání s daty získanými v rámci data retention, monitorovat.

Existují zhruba dva okruhy **argumentů v neprospěch** plošného uchovávání telekomunikačních dat, z nichž jeden se týká ochrany soukromí a druhý rozporu s principem proporcionality, malé efektivity a závažných důsledků pro ekonomiku. Předně se podobná opatření považují za **nepřípustný zásah do základního lidského práva na soukromí**, jak je definováno v příslušných ustanoveních mezinárodních smluv a v ústavních normách členských států EU. Z hlediska kriminalistického je totiž hlavním účelem data retention možné využití uložených dat k tzv. traffic analýze. Ta spočívá ve vizualizaci četnosti spojení mezi body sociální sítě, vyhodnocující změnu ve struktuře řídících či uzlových bodů takové sítě, četnost jejích aktivit a sílu vazeb mezi uzly.[23] Jinými slovy analytická centra tajných služeb či policejních orgánů dokáží na základě klasifikace sebraných metadat průběžně mapovat sociální síť každého občana, sledovat s kým a jak často komunikuje. Při vyhodnocení aktivit určité osoby na internetu pomocí traffic analysis lze ze zobrazených nebo stažených informací dovodit kulturní a politické preference či osobní zájmy a záliby. Zaznamenaná lokalizační data mobilních telefonů umožňují za optimálních podmínek dokonce sledovat pohyb jednotlivce.

Základní problém tkví v tom, že zatímco např. policejní odposlechy podle zákona postihují toliko osoby podezřelé z trestné činnosti, plošné schraňování dat vezme kontrolu nad osobními informacemi všem občanům *a priori*. I když není prozatím povinně ukládán obsah komunikace, sebraná metadata představují velmi detailní informace o životě každého uživatele. Vědomí, že jsou tyto údaje plošně ukládány a mohou být k dispozici i po dobu několika let, vytvoří nežádoucí atmosféru nedůvěry a obav ze zneužití. Občané se napříště nebudou moci spolehnout na anonymitu telefonní a elektronické komunikace a jejich životy naplní ponižující nejistota. Mnozí ve snaze vyhnout se rizikům raději upustí od společné komunikace skrze elektronické sítě. Nelze totiž vyloučit, že na základě chybného vyhodnocení dat bude docházet k podezírání nevinných občanů policií. Vznik tak rozsáhlých databází neúnosně zvyšuje riziko, že se údaje dostanou do nepovolaných rukou.[24] Kritici upozorňují na dopad zadržování dat např. na důvěrnou komunikaci s lékaři, psychoterapeuty, právníky, duchovními, novináři atd., jejichž potenciální klienti nebudou mít možnost je anonymně kontaktovat po telefonu či internetu. Data retention poskytne bezpečnostním orgánům státu nadmíru účinný nástroj politické kontroly, neboť umožní velmi podrobně monitorovat činnost a složení jakékoli protestní skupiny, i když se tyto aktivity pohybují v mezích zákona. I z tohoto důvodu je směrnici vytýkáno, že neobsahuje závazný výčet trestných činů, jejichž vyšetřování by odůvodňovalo vyžádání uložených dat.

Druhý okruh argumentů **zpochybňuje účinnost** směrnice v poměru k jejím závažným negativním dopadům. U části odborné veřejnosti panuje skepse, zda data retention pomůže při vyšetřování trestných činů. Pro organizovaný zločin i teroristy nebude zřejmě nijak obtížné zabránit, aby jejich komunikace byla zachycena, přičemž

[23] http://www.blisty.cz/art/27211.html

[24] Např. v USA již opakovaně došlo k případům, kdy policisté či zaměstnanci telekomunikačních společností prodávali cizí data soukromým agenturám. Odpůrci směrnice zejména varují před nebezpečím hospodářské špionáže. Blíže viz např. http://technology.guardian.co.uk/online/insideit/story/0,13270,1245613,00.html

technických možností jak toho docílit je celá řada a stále se rozšiřují. Např. již dnes nic nebrání např. kupovat SIM karty do mobilních telefonů u operátorů mimo Evropu a často je vyměňovat.[25] Možnosti v rámci sítě internet jsou ještě větší, závisí jen na výši finančních prostředků. Data retention tedy může ilegální aktivity jen trochu prodražit, ale skutečně efektivním nástrojem odhalování zločinu se nestane. Tato předpokládaná omezená účinnost je v příkrém kontrastu s obrovskými náklady, které si data retention v rozsahu určeném směrnicí vyžádá. I když budou náklady hrazeny telekomunikačním firmám z rozpočtu členských států, není vyloučeno, že se část firem pokusí povinnostem spojeným s data retention vyhnout a přesunou své působení do zemí bez takových požadavků, což občany EU připraví o pracovní místa.[26]

Lze se domnívat, že základním kritériem při posuzování nových evropských směrnic o uchovávání telekomunikačních dat by měl být soulad popř. nesoulad zaváděných opatření s **principem proporcionality**. Není sporu o tom, že schraňování dat a následná možnost získat velmi podrobné informace o libovolném uživateli elektronické komunikace představuje vážný zásah do práva na soukromí v tom smyslu, jak o něm bylo pojednáno v úvodu. Tam, kde mezinárodní úmluvy i prameny evropského práva umožňují orgánům státu zasáhnout do základních práv, vždy tak činí s podmínkou, že zásah bude přiměřený a zároveň nezbytný pro ochranu jiných důležitých práv a svobod (viz čl. 8 odst. 2 Úmluvy). Východiskem této úpravy je zásada, že jednotlivá základní práva jsou *prima facie* rovnocenná a jejich vzájemné zvažování, popř. upřednostnění jednoho právního statku před druhým je otázkou politické a filozofické argumentace v konkrétním případě. Společnost zpravidla dává přednost ochraně těch hodnot, které se v určitém dějinném okamžiku jeví více ohroženy nebo nedostatkové. Na toto vnímání priorit mají ovšem v moderní době nemalý vliv nejrůznější politické tlaky zájmových skupin a mediální manipulace.

Chceme-li správným způsobem řešit **kolizi mezi dvěma hodnotami či zájmy**, kdy ochrana jednoho z nich vyžaduje porušení druhého, měli bychom především vycházet z **kritéria vhodnosti**, tzn. posoudit, zda jsou opatření omezující určité základní právo ve prospěch práva jiného s to dosáhnout sledovaného cíle. Zároveň je třeba zvážit, zda není k dispozici jiný prostředek ochrany prioritního právního statku, který by druhý zájem buď nezasáhl, nebo jej zasáhl v menší míře.[27] Domnívám se, že zavedení povinného schraňování telekomunikačních dat, tak jak je požaduje nová evropská směrnice, nemůže být ospravedlněno na základě výše uvedených kritérií. Ze zkušenosti víme, že rozšiřování pravomocí bezpečnostních složek jen zřídka vede ke snížení kriminality, ale naopak hrozí narušením rovnováhy mezi pravomocemi státu a právy jednotlivce. Je zcela nepřiměřené uchovávat za cenu nesmírných nákladů ohromná množství telekomunikačních dat, bude-li v budoucnu užit pro účely vyšetřování jen nepatrný zlomek z nich. Jakkoli je právo na život a tudíž i právo na ochranu před případnými teroristickými útoky a zločinností právem nejzákladnějším, nic nenasvědču-

---

[25] http://www.bigbrotherawards.cz/nove_technologie_data_retention.html

[26] Více na http://wiki.ffii.de/DataRetVotePr051211En

[27] Srov. Pavlíček, V. a kol.: Ústavní právo a státověda, II. díl, Linde, Praha 2004, str. 73. Autor cituje nález Ústavního soudu ČR vyhl. pod č. 280/1996 Sb.

je tomu, že data retention výrazně zvýší bezpečnost občanů. Data retention je fenomén spojený se zcela disproporčními riziky a dopadem na celou společnost a její další směřování.

RIGHT TO PRIVACY VERSUS SECURITY IN THE UNIFIED EUROPE: CONSIDERATION ON THE PROBLEMS OF DATA RETENTION

Summary

The right to privacy is one of the fundamental rights guaranteed by both international conventions and the constitutional orders of nation states. Possible restrictions can be imposed only if they are necessary in a democratic society and if the principle of proportionality is observed. The storage of telephone and internet traffic and localization data for purposes of criminal investigation, usually referred to as data retention, is a new phenomenon which gives the government authorities access to the personal information of millions of citizens. By analyzing the retained data via traffic analysis the agencies can identify an individual's associates, habits, political preferences and even his or her location. Directive 2002/58/EC made it possible for several EU-Member States to pass laws that allow for personal telecommunication data to be stored for varied periods of time. In some countries data retention has been made compulsory for the telecommunications' providers. Although it had not been the case in Britain over the past few years, British providers store a large amount of data on a voluntary basis. In other countries such as Italy and France data retention laws have been in force for some time as an alleged means of combating terrorism and organized crime. In the Czech Republic too a new telecommunication law was adopted last year with provisions on data retention. However, the crucial step was taken only recently when the Data Retention Directive was adopted, which in fact forms a legal basis for the largest monitoring database in the world, tracking all communications within the EU. The opponents of the Directive see data retention as an invasion of privacy and a disproportionate response to the threat of terrorism – a measure both ineffective and harmful.

Key words: right to privacy, data retention, traffic analysis, mass surveillance