změny přijaty měla být vynucována implementace Směrnice po státech, které zatím (a nebo už) národní úpravou nedisponují. Tyto státy by pak měly zvážit, zda do vyřešení výše nastíněných problémů, budou pokračovat v přípravě národní implementace. To je v současné době i případ České republiky.

Data Retention ve Spojených státech

Eva Fialová [1]*

Abstrakt:
Častým argumentem odpůrců evropské směrnice o data retention je neexistence uchovávání provozních a lokalizačních údajů ve Spojených státech. V USA skutečně jednotná zákonná úprava data retention neexistuje. Povinnost uchovávat údaje je upravena zvláštními zákony. I když je pravdou, že některé údaje uchovávány být nemusí, již několikrát byl předložen návrh zákona, jenž povinnosti poskytovatelů významně rozšiřuje. Tento příspěvek se bude zabývat právní úpravou data retention ve Spojených státech.

Abstract:
Opponents of European Data Retention Directive frequently claim the non-existence of retention of traffic and localization data in the United States. In USA there does not exist a cohesive legal regulation of the data retention. The obligation is laid down by particular acts. Albeit, some data need not to be retained, the Congress introduced a bill significantly extending the obligations of providers. This paper deals with the legal regulation of the data retention in the United States.

Klíčová slova:
Data retention, Spojené státy

Keywords:
Data Retention, The United States

I. Úvod

Uchovávání provozních a lokalizačních údajů neboli data retention je v současné době nejen v České republice, ale i v dalších státech Evropské unie intenzivně diskutované téma, jež vyvolává emoce na straně zastánců i odpůrců. Právní úprava uchovávání údajů o uskutečněném telefonním či internetovém spojení nedoznává změn pouze v Evropě, nýbrž i ve Spojených státech amerických. V těchto měsících čeká v Kongresu na schválení již druhý návrh zákona přikazující poskytovatelům internetových služeb uchovávat údaje o internetové komunikaci. Tento článek se zabývá platnou právní úpravou data retention ve Spojených státech a legislativními návrhy mající za cíl povinné uchovávání rozšířit o další údaje.

II. Ochrana soukromí a osobních údajů v USA

Nejprve je třeba zmínit, že zásahy vlády (*government*) do soukromí jednotlivce jsou vnímána jako větší ohrožení svobody jednotlivce než zásahy soukromými subjekty.[2] Ústavně není právo soukromí výslovně zakotveno. Ochrana soukromí se odvozuje ze Čtvrtého dodatku Ústavy Spojených států. Podle něho nesmí být osobní, domovní svoboda, písemnosti a majetek narušovány neoprávněnými prohlídkami a zabavováním.[3]

Nejvyšší soud Spojených států již několikrát posuzoval ústavnost zpracovávání údajů vztahujících se k určité osobě. V případu *United States v. Miller*[4] rozhodoval Nejvyšší soud o ústavní ochraně bankovních údajů, jenž banka poskytla státním orgánům vedoucím trestní řízení proti panu Millerovi z důvodu krácení daně. Podle soudu nemůže mít ten, kdo svěří informace, jež nejsou označeny jako důvěrné, třetí osobě, ve vztahu k těmto informacím legitimní očekávání soukromí (*legitimate expectation of privacy*). Takovéto informace nepožívají ochrany Čtvrtým dodatkem.

Čtvrtý dodatek se nevztahuje ani na čísla vytáčená uživatelem telefonní stanice. Nejvyšší soud o tom rozhodl v případu *Smith v. Maryland*,[5] jenž se týkal otázky oprávněnosti zaznamenávání volaných telefonních čísel telefonní společností na žádost státního orgánu. Ani ve vztahu k vytáčeným číslům neexistuje legitimní očekávání soukromí.

Legitimní očekávání soukromí nemůže mít ani majitel mobilního telefonu. Podle *U.S. District Court for the District of Columbia* si rozumný spotřebitel musí být vědom skutečnosti, že se mobilní telefon připojuje k různým anténám. Díky tomu si musí také uvědomovat, že poskytovatel má přesné údaje o poloze konkrétního telefonu. Údaje o poloze mobilního zařízení analogicky k případu Smith v. Maryland nespadají pod ochranu Čtvrtého dodatku. Z toho podle soudu vyplývá, že státní orgány nemusí mít k jejich získání zvláštní povolení (*search warrant*).[6]

Zde je na místě poznamenat, že český Ústavní soud se k soukromé povaze údajů o telefonické komunikaci vyjádřil v opačném smyslu. Podle něj je soukromí každého člověka hodno ochrany nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům. Článek 13 Listiny zakládá podle Ústavního soudu ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho trvání a v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor.[7]

Zatímco tedy zpracovávání osobních údajů ve veřejném sektoru podléhá zákonným normám,

* evafialova@mail.muni.cz, ÚPT PrF MU

1 Příspěvek byl přednesen v rámci konference České právo a informační technologie 2011.

2 WHITMAN, J.Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal.* 2004, sv. 113, s. 81.
Dostupné z: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041>.

3 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

4 United States v. Miller 425 U. S. 435 (1976).

5 Smith v. Maryland 442 U. S. 735 (1979).

6 U.S. District Court for the District of Columbia, Misc. No. 11-449 (JMF/RCL) ze dne 3. října 2011.

7 IV.ÚS 1556/07.

v soukromém sektoru jsou pravidla pro toto zpracovávání předmětem samoregulace (*self-regulation*).

Není účelem tohoto článku podat detailní přehled celé legislativy upravující zpracovávání osobních údajů ve Spojených státech. Proto zde budou zmíněny pouze základní předpisy. Zpracovávání osobních údajů ve veřejném sektoru je upraveno primárně zákonem nazvaném *Privacy Act*. Dalším důležitým zákonem regulující zpracovávání údajů ve veřejném sektoru je *Electronic Communication Privacy Act*. Tento zákon upravuje odposlouchávání telefonních hovorů, používání zařízení pro záznam příchozích a odchozích telefonních čísel, emailových a IP adres a v neposlední řadě uchovávání údajů o komunikaci a její obsah.

Zatímco tedy zpracovávání osobních údajů ve veřejném sektoru podléhá zákonným normám, v soukromém sektoru jsou tato pravidla nastavena převážně samoregulací (*self-regulation*).[8] I v soukromém sektoru však existuje řada zákonných předpisů týkající se ochrany osobních údajů. Nejdůležitější z nich jsou *Children´s Online Privacy Protection Act*, jenž reguluje údaje získané od dětských uživatelů internetu, *Video Privacy Protection Act* chránící údaje o videích půjčených konkrétní osobou a *Telephone Consumer Protection Act*, v němž jsou stanovena pravidla pro tzv. telemarketing.

III. Uchovávání údajů o komunikaci

Ve Spojených státech neexistuje právní předpis srovnatelný s evropskou směrnicí o data retention č. 2006/24/ES, který by ukládal poskytovateli telefonního či internetového připojení nebo služby obecnou povinnost uchovávat údaje o telefonní a internetové komunikaci. Neexistuje však ani povinnost údaje mazat či anonymizovat.

Uchovávání údajů je stanoveno zvláštními zákony a je vázáno na účel těmito zákony stanovený. Prvním z nic je *Code of Federal Regulation* (dále: CFR), čili Sbírka federálních nařízení správněprávní povahy. Podle § 42.6 CFR musí poskytovatelé telefonních služeb uchovávat po dobu 18 měsíců údaje nutné pro fakturaci. Uchovávaným údajem je jméno, adresa, telefonní číslo volajícího a volaného, datum, čas a délka hovoru.

Další údaje může poskytovatel uchovávat, pokud je specifikoval v tzv. vzorovém seznamu údajů (*master index of records*). V seznamu musí poskytovatel uvést druh údaje, dobu uchovávání a místo, kde je údaj uchováván. Tento seznam podléhá přezkumu Federální komisí pro komunikace (*Federal Communication Commission*). Podle § 42.4 CFR může Komise nařídit poskytovateli, aby do seznamu přidal další údaje, či prodloužil dobu uchovávání.

Code of Federal Regulation nestanoví povinnost smazat nebo anonymizovat údaje po uplynutí doby, po kterou musí být údaje uchovávány.

Dalším předpisem, jenž upravuje uchovávání údajů a hlavně pravidla pro jejich předávání státním orgánům, je již zmíněný Electronic Communication Privacy Act (dále: ECPA), respektive druhý titul tohoto zákona nazvaný *Stored Wire and Electronic Communications Transactional Records Access*. ECPA poskytuje ochranu telefonní, slovní a elektronické komunikaci (*wire, oral and communication*).

Podle § 2703(c) ECPA může státní orgán (*governmenal entity*) žádat poskytovatele komunikační služby nebo služby dálkového přístupu (*remote computing*), aby poskytl údaje o uživateli (*a record or other information pertaining to a subscriber to or customer*), vyjma obsahu komunikace. Státní orgán může údaje získat na základě povolení (*warrant*), soudního příkazu (*court order*), obsílky (*subpoena*) nebo, v případě podvodu v oblasti telemarketingu, na základě písemné žádosti předložené poskytovateli, jehož předplatitel je z podvodu podezřelý. Mimo výše uvedených prostředků může k předání údajů dát souhlas sám předplatitel komunikační služby.

Kromě souhlasu předplatitele je nejrychlejším a nejméně formalizovaným způsobem k získání údajů o komunikaci administrativní obsílka (*administrative subpoena*), kterou jsou oprávněné vydat státní orgány domáhající se vydání určitého dokumentu či svědectví.[9] Podle ECPA mohou státní orgány tímto relativně jednoduchým způsobem získat jméno a adresu předplatitele, údaje o lokálním a dálkovém telefonickém spojení a o času a délce spojení. Dalšími údaji, které lze tímto způsobem získat jsou údaje o délce poskytování služby a typu služby, telefonní číslo a číslo přístroje nebo jiné uživatelské číslo či uživatelská identita, včetně dočasně přidělené adresy. Obsílka může dále zahrnovat povinnost poskytovatele sdělit státnímu orgánu prostředky a zdroje platby za službu, včetně čísla kreditní karty nebo čísla účtu. Seznam údajů byl značně rozšířen po vydání tzv. *Patriot Act*, jenž byl reakcí na útoky na World Trade Centre 11. září 2001. Tímto zákonem dostaly státní orgány oprávnění získat formou obsílky údaje o času a délce spojení, údaje o uživatelské identitě a dočasně přidělené adrese a hlavně o údaje o prostředcích a zdrojích platby za komunikační službu.

Dalším prostředkem k získání údajů uchovávaných poskytovateli je podle ECPA soudní příkaz. Soudní příkaz vydá soud pouze, pokud se požadované údaje vztahují k probíhajícímu vyšetřování. Soud může příkaz zrušit nebo změnit, pokud je množství požadovaných údajů neobvykle velké či pokud by vyhovění soudnímu příkazu znamenalo pro poskytovatele značnou zátěž. Zajímavostí je, že zákon výslovně zakazuje podat žalobu proti poskytovateli z důvodu poskytnutí údajů státnímu orgánu.

ECPA zná pouze jeden případ uchovávání údajů, jenž by mohly sloužit jako důkazy potřebné k vydání soudního příkazu či pro jiné řízení. Poskytovatel komunikační služby má na žádost státního orgánu podle §2703(f) povinnost uchovávat údaje a další důkazy (*records and other evidence*) vztahující se ke konkrétnímu

8 BLOK, P. Het recht op privacy: een onderzoek naar een onderzoek naar de betekenis van het begrip privacy in het Nederlandse en Amerikaanse recht. (Právo na soukromí: výzkum pojmu soukromí v nizozemském a americkém právu). Den Haag: Boom Juridische Uigevers, 2002. s. 208.

9 Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities. *U.S. Department of Justice* [online]. [cit. 2011-09-21].
Dostupné z <http://www.justice.gov/archive/olp/rpt_to_congress.htm>.

vyšetřování. Doba uchovávání údajů je stanovená na 90 dnů s možností prodloužení o dalších 90 dnů.

IV. Uchovávání de lege ferenda

Na poskytovatele internetových služeb (ISP) se povinnost uchovávat údaje o komunikaci při využívání jejich služeb doposud nevztahuje. Vláda Spojených států se ovšem již další dobu snaží tuto situaci změnit. Oficiálním důvodem připravované legislativy je potírání dětské pornografie na internetu.

První návrh zákona byl předložen v roce 2009 pod názvem *Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (Safety Act)*.[10] ISP měli podle tohoto návrhu uchovávat údaje (*records*) a jiné informace o identitě uživatele minimálně po dobu dvou let. Pro srovnání je třeba dodat, že tato doba koresponduje s maximální dobou pro uchovávání podle evropské Směrnice o data retention.

V první polovině roku 2011 byl spatřil světlo v pořadí druhý návrh nazvaný *Protecting Children from Internet Pornographers Act*.[11] Podle původního návrhu měl ISP uchovávat údaje o dočasně přidělené adrese po dobu minimálně 18 měsíců. Tato doba byla stanovená analogicky k uchovávání fakturačních údajů podle CFR.[12] Po vlně kritiky, která se proti návrhu zvedla,[13] změnila Komise pro soudnictví (*Committee on the Judiciary*) v návrhu jak povinně uchovávané údaje, tak i dobu, po kterou se budou údaje uchovávat.Pokud tento návrh projde legislativním procesem, budou ISP uchovávat místo údajů o dočasně přidělované adrese jméno a adresu uživatele, IP adresu, číslo bankovního účtu a číslo kreditní karty plátce služby. Minimální retenční doba se z 18 měsíců zkrátila na jeden rok.[14]

V. Závěr

Právní úprava data retention není ve Spojených státech obsažena v jednom právním předpise. Plošné uchovávání údajů o telefonické a internetové komunikaci analogické evropské směrnici č. 2006/24/ES americký právní řád nezná. Poskytovatelé mají povinnost uchovávat pouze údaje potřebné pro fakturaci telekomunikační služby a údaje, jenž mohou sloužit státnímu orgánu jako důkazy během probíhajícího vyšetřování.

Kdo a za jakých podmínek má oprávnění údaje, které mají poskytovatelé k dispozici, požadovat, stanoví Electronic Communication Privacy Act. Nejrychlejším a nejméně formalizovaným způsobem je vydání administrativní obsílky, za základě které může státní orgán získat i informace o platbě za službu včetně čísla kreditní karty či čísla účtu. Oproti evropské právní úpravě, neobsahuje ECPA pravidla pro smazání nebo anonymizaci údajů.

V současné době se ve Spojených státech vede debata o návrhu zákona proti dětské pornografii na internetu. Pokud tento návrh vstoupí v platnost, budou muset ISP uchovávat všechny zákonem stanovené údaje minimálně po dobu jednoho roku.

10 H.R.1076 Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009. *The Library of Congress* [online]. [cit. 2011-09-23]. Dostupné z: <http://thomas.loc.gov/cgi-bin/query/D?c111:5:./temp/~c111KvvSCW::#/>.

11 H.R.1981 Protecting Children From Internet Pornographers Act of 2011. *The Library of Congress* [online]. [cit. 2011-09-21].

12 Statement of Judiciary Committee Chairman Lamar Smith Subcommittee on Crime, Terrorism and Homeland Security Hearing on H.R. 1981, the „Protecting Children from Internet Pornographers Act of 2011". *Committee on the Judiciary* [online]. Vydáno 12. července 2011. [cit. 2011-10-11]. Dostupné z: <http://judiciary.house.gov/news/Statement%20HR%201981.html>.

13 např. FRIEDERSDORF, C. The Legislation That Could Kill Internet Privacy for Good. *The Atlantic* [online]. Vydáno 1. srpna 2011. [cit. 2011-09-20]. Dostupné z: <http://www.theatlantic.com/politics/archive/2011/08/the-legislation-that-could-kill-internet-privacy-for-good/242853/>.

14 ASWORD, W. US approves ISP data retention bill. *Computer Weekly* [online]. Vydáno 29. července 2011. [cit. 2011-09-20]. Dostupné z: <http://www.computerweekly.com/Articles/2011/07/29/247452/US-approves-ISP-data-retention-bill.htm>.