Projekt pracuje s osobními údaji o zdraví každé osoby. Jak řešíte otázku ochrany těchto dat?
Využíváme formuláře pro informovaný souhlas. Pacienti musí podepsat dohodu, aby byla uvolněna jejich data pro tento konkrétní druh výzkumu. Existuje speciální nástroj zvaný CAT, který užívá kryptografické metody a anonymizuje údaje o pacientech. Tato data jsou poté vložena do nové databáze, která je kopií databáze v nemocnici. Takzvané databáze přístupné v síti (grid-accessible databases) obsahují de facto anonymní data, čímž splníme směrnici o ochraně osobních údajů. Genetické údaje jsou totiž považovány za unikátní, ale také velice citlivé. Z tohoto důvodu musíme chránit pacientovo právo na soukromí.

Je zde nějaká možnost, že by pacientovi přítomnost jeho dat v databázi mohla pomoct s léčbou?
Je přímo naším cílem umožnit návrat ke konkrétnímu pacientovi nebo ke komunitě pacientů, když nalezneme jakýkoli lék pro konkrétní druh rakoviny.

Takže v případě, že je nalezen lék pro nějaký konkrétní případ v databázi, existuje možnost pomoci konkrétnímu pacientovi?
Lze předpokládat, že to možné bude, ale v současné době jsme s touto možností ještě nepracovali, protože projekt není zatím dokončen. Chtěli bychom se alespoň vracet ke komunitám pacientů. Se zdravotními daty pacientů nelze obchodovat jako se zbožím, proto pacientům nemůžeme vyplácet peněžní odměnu z prostředků získaných díky výzkumu, který svými daty umožnili. Náš projekt můžeme porovnat s projektem lidského genomu, který pracuje s návratností několika procent, konkrétně jedno až tři procenta z příjmů projektu. My jsme zvýšili procentní návratnost na tři až pět procent. Proto bychom se rádi pacientům odvděčili prostředky v hodnotě uvedených procent z našich příjmů pomocí nového druhu léčby nebo zlepšení v jejich nemocnici nebo v komunitě, která se zúčastnila těchto klinických zkoušek.

Zmínil jste, že vaše síťová výpočetní infrastruktura má více či méně vrstev, ve kterých pracuje. Můžete to vysvětlit?
Síťová infrastruktura je velice komplexní a je to poměrně nový koncept. Je rozdělena do tří různých vrstev. Nejnižší vrstva je nazývaná Platforma (the Platform), kde můžete nalézt hardware a síťovou infrastrukturu, například počítačovou infrastrukturu státu, třeba Řecka, Belgie či Velké Británie. Pak je zde střední vrstva, která je složena z kteréhokoli počítačového softwaru, jehož účelem je usnadnit přístup k datům. V této vrstvě přicházíme zpět ke včelí metafoře. Podobně jako včely komunikují prostřednictvím tance, tedy nejjednodušším způsobem, jak jedna včelí dělnice může říct druhé, kde lze nalézt květiny okolo úlu, my v této vrstvě říkáme našim pacientům, kde můžou nalézt důležité informace. Třetí vrstva se nazývá Přihláška uživatele a v zásadě ji tvoří webová stránka využívající sémantického webu a sémantických nástrojů.

Jaké jsou základní právní otázky a problémy, které jsou spojeny s tímto projektem?
Je zde mnoho právních otázek a problémů, zejména zmíněná ochrana osobních údajů a také otázka duševního vlastnictví. V projektu totiž figuruje nepřeberné množství jednotlivých práv k patentům, autorských práv a práv pořizovatele databází.

V prezentaci vašeho projektu byla zmíněna s ním spojená síť důvěry. Kdo budou členové této sítě důvěry?
Síť důvěry je otevřená komukoli. Je přístupná každému výzkumníkovi, který by chtěl provádět výzkum rakoviny. Síť důvěry se skládá zejména z hlavních dotčených skupin subjektů, což jsou pacienti, lékaři, výzkumníci a koncoví uživatelé. Důležitou úlohu v rámci projektu má Centrum pro ochranu osobních údajů (Center of Data Protection), které shromažďuje dohody s pacienty, kteří musí podepsat formulář souhlasu s uvolněním dat, a s koncovými uživateli, kteří musí podepsat dohodu, aby získali přístup k těmto datům. Centrum funguje uvnitř projektového rámce jako nevládní nezisková organizace, ale je otevřené komukoli. Lze je využít k založení jakéhokoli projektu. Organizace má technického partnera CUSTODIX, který je pověřen zabezpečením dat, a další dva partnery v oblasti práva. Prezidentem Centra je profesor Nikolaus Forgó, který je také zástupcem ředitele celého našeho institutu.

Chtěl byste ještě přidat nějakou informaci na závěr?
Chtěl bych vyslat následující vzkaz: u tohoto typu výzkumu potřebujeme najít rovnováhu mezi všemi zúčastněnými subjekty včetně pacientů. Zejména skupina pacientů je opravdu důležitá, protože právě díky nim může být náš projekt přínosný. Potřebujeme jejich údaje, aby bylo možné provádět zdravotnický výzkum. A čím více údajů nasbíráme, tím větší je pravděpodobnost, že nalezneme nějaký lék na rakovinu.

Profil osoby: Marcelo Corrales, LL.M.
http://www.iri.uni-hannover.de/corrales.html

Marcelo Corrales, LL.M.

Rozhovor vedl: Mgr. Bc. Libor Kyncl, Ústav práva a technologií, Právnická fakulta, Masarykova univerzita

Aktuální otázky data retention

Matěj Myška

O tzv. data retention se debatovalo 26. května v prostorách Právnické fakulty Masarykovy univerzity. Výstižný a hlavně úderný český ekvivalent tohoto zažitého anglického výrazu by se asi hledal těžko, slovy zákona[1] se jedná o *„povinnost osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací*". Uchovávání dat je poměrně složitá problematika, která však není příliš populární ani medializovaná. Má ovšem enormní praktický dopad na každého jednotlivce.

Laicky řečeno: operátoři a poskytovatelé připojení k internetu mají povinnost po dobu 6 měsíců uchovávat údaje o uskutečněných hovorech a internetovém provozu

Mgr. Matěj Myška

jednotlivce, a to bez speciálního důvodu a účelu. Plošně se tak uchovávají informace o tom, kdo, kdy, komu, z jakého přístroje a z jakého místa volal, či posílal SMS zprávy. U internetových služeb se kromě základních identifikačních údajů počítače uživatele a serveru uchovává i množství přenesených dat, v případě e-mailu i takové podrobnosti, jako např. zda byla komunikace šifrována. Přestože je striktně zakázáno uchovávat obsah komunikace, dostala se problematika data retention do hledáčku nevládních organizací, zabývajících se ochranou lidských práv. Jak samotný princip bezdůvodného konstantního uchovávání komunikačních údajů, tak i šíře a záběr takto uchovávaných údajů, je dle jejich názoru nutné považovat za neproporcionální zásah do základního lidského práva na ochranu soukromí, potažmo telekomunikačního tajemství. V mnoha zemích EU iniciovaly tyto organizace ústavněprávní přezkum dotčených předpisů upravujících data retention.

Zejména na tyto problematické aspekty právní úpravy data retention se zaměřil i workshop s názvem Aktuální otázky data retention. Cílem workshopu mělo být také vyplnit mezeru v doposud chybějící české odborné debatě na toto téma. Nejprve se ve

1 Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.

své úvodní přednášce Mgr. Myška, asistent na Ústavu práva a technologií, věnoval historickému vývoji konceptu uchovávání provozních a lokalizačních údajů. Poté představil úpravu ve směrnici 2006/24/ES[2] a věnoval se problematickému procesu přijímání této směrnice a zpochybňované volbě právního základu jejího přijetí[3]. Následně se zaměřil na úpravu v českém zákoně o elektronických komunikacích a prováděcích vyhláškách ministerstva informatiky č. 485/2005 Sb. a Českého telekomunikačního úřadu č. 486/2005 Sb. Hlavním tématem jeho přednášky však byla analýza návrhu Ústavnímu soudu (ÚS) na zrušení české úpravy data retention a rozhodnutí německého Spolkového ústavního soudu o ústavnosti data retention.

Data retention před českým Ústavním soudem

Iniciátorem českého návrhu[4], který dne 17. března 2010 podala skupina poslanců Parlamentu ČR, byla organizace Iuridicum Remedium. Poslanci, zastoupeni Markem Bendou, tvrdí, že napadená ustanovení zákona o elektronických komunikacích a prováděcí vyhláška zasahují do základních práv na ochranu soukromého života, na ochranu před neoprávněným shromažďováním údajů o své osobě a na ochranu telekomunikačního tajemství zakotvených v čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13 Listiny základních práv a svobod a čl. 8 Úmluvy o ochraně lidských práv a základních svobod.

V první části návrhu je řešena otázka, zda provozní a lokalizační údaje spadají pod ochranu výše uvedených článků a zda se v případě data retention skutečně jedná o zásah do zmíněných základních práv. Poukazem na judikaturu ÚS[5] a Evropského soudu pro lidská práva[6] dospívají navrhovatelé k závěru, že data retention je nutné kvalifikovat jako relevantní zásah, a to jednak konkrétní, ale i potenciální. Předpokladem dovolenosti zásahu je jeho přiměřenost vzhledem k významu daného práva. Dále je nutné, aby byl odůvodněn naléhavou společenskou potřebností a byl proporcionální vzhledem k sledovanému legitimnímu cíli. Právě nepřiměřenost právní úpravy data retention je vytýkána v druhé části návrhu.

Z hlediska závažnosti a rozsahu zásahu poukazují navrhovatelé na extrémní rozsah a šíři uchovávaných údajů. Častým argumentem zastánců data retention je, že provozní a lokalizační údaje *per se* představují kvalitativně méně intenzivní zásah do práv subjektu, vzhledem k tomu, že není uchováván samotný obsah komunikace. Toto navrhovatelé vyvrací poukazem na zvýšenou možnost automatického zpracování údajů. Zatímco vyhodnocovat odposlechy telekomunikačního provozu musí stále provádět fyzická osoba, z uchovaných dat lze pomocí sofistikovaných programů vytvářet např. tzv. „komunikační profily" jednotlivce. Z pak nich lze s vysokou pravděpodobností dovozovat i samotný obsah komunikace. Dají se ale použít např. k identifikaci sociálních vazeb jednotlivce či např. k rozkrývání hierarchických vazeb v organizacích. Nevyhovující je i značný okruh orgánů státní moci, které mají k uchovávaným datům přístup. Z hlediska legitimity a cíle a přínosu zásahu k dosažení tohoto cíle uvádějí navrhovatelé zejména neprokázanou korelaci mezi zavedením data retention a zvýšením objasněnosti trestných činů. Konečně navrhovatelé upozorňují na možnost nebezpečí jak zneužití, tak až příliš extenzivního využívání shromažďovaných údajů, zejména za současného stavu, *„kdy nejsou podrobně vymezeny podmínky, za kterých může dojít k jejich využívání"*[7].

Navrhovatelé své posuzování proporcionality uzavírají konstatováním, že v případě data retention se jedná o zásah do základních práv dotčených osob, a to konkrétně zásah takový, který je s cílem a pravděpodobným a očekávatelným užitkem z uchovávaných údajů v hrubém nepoměru. Nadto uvádějí, že data retention je samo o sobě prostředkem málo efektivním, jelikož pachatelům trestné činnosti jsou stále k dispozici možnosti, jak svoji komunikaci anonymizovat. V závěru návrhu dávají poslanci Ústavnímu soudu ke zvážení i předložení předběžné otázky Evropskému soudnímu dvoru, jelikož zde *„existuje významné riziko, že samotná Směrnice je neplatná z hlediska práva Evropských Společenství, a to z důvodu jejího rozporu se základními právy Společenství, a to z důvodu jejího rozporu se základními právy Společenství"*.[8] S tímto též úzce souvisí i problematika přezkumu ústavnosti transpozičních ustanovení. Na rozhodnutí Ústavního soudu ve věci se spisovou značkou Pl. ÚS 24/10 si však nejspíše nějakou chvíli počkáme, jak ostatně potvrdil na webových stránkách soudu jeho generální sekretář Tomáš Langášek: *„Délku řízení ani výsledek pochopitelně předjímat v tuto chvíli nelze."*

IURIDICUM REMEDIUM

Občanské sdružení Iuridicum Remedium (IuRe) je nevládní organizace typu watchdog, která vznikla původně jako iniciativa studentů pražské právnické fakulty. Jak uvádí na svých webových stránkách www.slidilove.cz: *„Posláním IuRe je aktivně přispívat spolu s dalšími organizacemi a občany k dodržování základních práv a svobod a bránit jejich omezování pod nejrůznějšími záminkami (boj s terorismem, kriminalitou apod.)."* Sdružení také uděluje českou mutaci „Big Brother Award", tedy cenu pro subjekt, který nejvíce narušuje soukromí občanů, zejména použitím moderních technologií. Další informace o sdružení a jejich aktivitách jsou dostupné na www.iure.org a www.bigbrothersawards.cz.

Rozhodnutí německého Spolkového ústavního soudu

Výsledek předjímat opravdu nelze, lze se však podívat na judikaturu zahraniční, konkrétně německou. Rozbor ústavní stížnosti a hlavně rozhodnutí o ní bylo dalším tématem přednášky Mgr. Myšky. Ústavní stížnost, kterou iniciovala Pracovní skupina Vorratsdatenspeicherung, byla podána u Spolkového ústavního soudu v Karlsruhe již 31. prosince 2007. Napadány byly §§ 113a a 113b německého telekomunikačního zákona a §110a německého trestního řádu, stanovující poskytovatelům veřejně dostupných telekomunikačních služeb povinnost plošně uchovávat údaje o telekomunikačním provozu po dobu 6 měsíců. Podle stěžovatelů představuje takovéto plošné uchovávání nepřiměřený zásah do práva na soukromí, práva na ochranu telekomunikačního tajemství a práva na informační sebeurčení.

Soud judikoval, že uchovávání údajů samo o sobě protiústavní není, a to přesto, že se jedná o *„obzvláště závažný zásah s dopadem, jaký německý právní řád doposud nepoznal"*. Rozhodujícím pro dovolenost data retention je dle soudu časové omezení uchovávání údajů. Čas, po který jsou data uchovávána, je omezený[9] na dobu šesti měsíců. I když je to dle soudu poměrně dlouhá doba, je ještě přípustná – po půl roce se tak občan může spolehnout na to, že uchovaná data budou nenávratně smazána. Dalším důvodem přiměřenosti úpravy data retention je fakt, že data nejsou uchovávána přímo státem, ale za pomoci soukromých subjektů, poskytovatelů služeb elektronických komunikací, a to partikulárně – stát tak nemá přístup ke všem potřebným datům najednou jako k balíku dat. Nevzniká tedy jakýsi univerzální data pool, ke kterému by měly státní složky neomezený přístup. Samotný zásah do základních práv je tedy podle německého Spolkového ústavního soudu pro stíhání trestných činů a odvracení nebezpečí nutno považovat za přiměřený. Vzhledem k intenzitě takového zásahu je ale předpokladem ústavněprávní konformity právní úpravy data retention vyhovění specifickým požadavkům.

Předně se jedná o požadavek na legislativní zakotvení zvýšené úrovně zabezpečení

2 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.

3 K tomu více vizte rozhodnutí Evropského soudního dvora ve věci C-301/06.

4 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 (dále jen „Návrh"). Kompletní text návrhu dostupný z: http://www.concourt.cz/clanek/GetFile?id=3121.

5 Zejména nález Ústavního soudu sp. zn. II ÚS 502/2000.

6 Rozhodnutí ESLP ve věcech Klass v. Německo, P. G. aj. H. v. Spojené království, Amann v. Švýcarsko, Copland v. Spojené království

7 Návrh, str. 16.

8 Tamtéž, str. 19.

9 Naopak již dříve německý soud judikoval, že uchovávání dat bez časového omezení je protiústavní.

uchovávaných dat. Ke kritériu bezpečnosti konstatovali soudci 1. senátu, že v napadených zákonech odkazuje pouze na obvyklou pečlivost v oboru poskytování služeb elektronických komunikací. V zákoně tak není zakotven žádný způsob, jak na subjektech povinných uchovávat data vymoci potřebný vysoký standard zabezpečení (bezpečné oddělené uchovávání dat, asymetrické šifrování, aplikace two-man rule atd.). Dále soudci podotknuli, že podnikatelé působící v oboru nabízejí své služby za podmínek konkurenčního boje o zákazníka a cenové války, a nebudou tedy dodržovat nákladnější bezpečnost. Stejně tak chybí vyvážený a účinný systém sankcí za porušení takovýchto požadavků na bezpečnost. Nutná je dále i jasná a srozumitelná regulace přístupu k uchovávaným údajům, jakož i transparentnost při nakládaní se shromážděnými daty. Soud zde zmínil i požadavek alespoň dodatečného vyrozumění subjektu, jehož uchované údaje byly použity. Konečně je nutno poskytnout jednotlivci i dostatečnou právní ochranu, tedy možnost obrátit se na soud s žádostí o přezkum využití uchovaných údajů. Tyto výše uvedené požadavky ovšem *in concreto* dosavadní německá úprava nenaplňovala, a proto byla soudem prohlášena za protiústavní. Příslušná ustanovení však nebyla zrušena, soud pouze pozastavil jejich účinnost. Zároveň nařídil okamžité smazání údajů nashromážděných na základě napadených ustanovení.

Arbeitskreis Vorratsdatenspeicherung

Pracovní skupina Vorratsdatenspeicherung je největší německou občanskou iniciativou namířenou proti uchovávání provozních a lokalizačních údajů fungující od prosince 2005. Toto neformální sdružení právníků, ochránců lidských práv a aktivistů iniciovalo též hromadnou ústavní stížnost proti implementaci směrnice 2006/24/ES do německého právního řádu. Na webových stránkách iniciativy www.vorratsdatenspeicherung.de je dostupná veškerá dokumentace k řízení o ústavní stížnosti před německým Spolkovým ústavním soudem, jakož i další relevantní informace a zdroje k tématu data retention.

Obdobně jako v návrhu českých poslanců byl soud požádán i o položení předběžné otázky k Evropskému soudnímu dvoru a s tím související přezkoumání platnosti samotné směrnice z hlediska možného zásahu do základních lidských práv. Toto však soud neučinil a konstatoval, že směrnici bylo možno provést, při splnění výše uvedených požadavků, v souladu s německým Základním zákonem, a tím pádem zde není důvod předkládat předběžnou otázku Evropskému soudnímu dvoru. Jak zdůraznil Mgr. Myška na konci své přednášky: „*Povinnost uchovávat údaje bude tedy v Německu opět zavedena, i když v jiné než v dosavadní podobě.*“

Data retention v ostatních zemích EU

Právní úprava data retention byla podrobena ústavněprávnímu přezkumu i v ostatních zemích Evropské unie. Rozbor těchto rozhodnutí, konkrétně rumunského Ústavního soudu a bulharského Nejvyššího správního soudu přinesl příspěvek Mgr. Rastislava Guľaši, interního doktoranda na Katedře ekonomických věd a práva informačních a komunikačních technologií Právnické fakulty Univerzity Komenského v Bratislavě.

Rumunsko

Rumunský Ústavní soud zrušil rozhodnutím č. 1258/2009[10] ustanovení zákona č. 298/2008, o uchovávaní údajů vytvořených a zpracovaných poskytovateli veřejných elektronických komunikačních sítí a služeb, a zákona č. 506/2004, o zpracovaní osobních údajů a ochraně soukromí v sektoru elektronických komunikací. Impuls pro přezkoumání vyšel opět od nevládní organizace, konkrétně od Komisariátu občanské společnosti, která

Mgr. Rastislav Guľaša

ve svém podnětu namítala rozpor uvedených předpisů s ustanoveními rumunské ústavy, Všeobecné deklarace lidských práv a konečně Úmluvy. Rumunský ústavní soud konstatoval ve svém rozhodnutí několik důvodů, pro které jsou napadené zákony protiústavní. Jedná se zejména o neurčitost pojmu „související údaje“, resp. „related data“, které se mají taktéž uchovávat a poskytovat státním orgánům. Nejasnost tohoto pojmu podle soudu způsobuje nejistotu subjektů o tom, které údaje jsou o nich ve skutečnosti uchovávány, a navíc to otevírá další možnosti jejich zneužití. Dalším nedostatkem je nejasnost úlohy „národní bezpečnosti“, v souvislosti se kterou se mají údaje uchovávat a zpřístupňovat, což opět způsobuje právní nejistotu a může skončit nepřiměřeným sledováním aktivit občanů ze strany státu. Ústavní soud dále konstatoval, že plošné a dlouhodobé uchovávání údajů je v rozporu se zásadou ochrany osobních údajů a v takové míře je neproporcionální. Nemůže tak být považováno za výjimku ze zásady a odůvodňovat plošný zásah do ústavou chráněných práv občanů. Na závěr soud uvedl, že nepopírá legitimitu přijetí zákona, podle kterého by se měla data retention realizovat. Vyjádřil však požadavek, že takovýto zákon by měl vytvořit spolehlivé právní nástroje na ochranu ústavních práv a měl by zohledňovat současný technický vývoj a možnosti. Ústavní soud v závěru svého rozhodnutí uznal, že ochrana lidských práv nemůže jít „ad absurdum“, ale zdůrazňuje, že výjimky z ochrany musí být řádně zdůvodněné a přiměřené cílům.

10 Rozhodnutí ze dne 8. 10. 2009, dostupné z: http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf.

Bulharsko

I v Bulharsku vzešla iniciativa z nevládního sektoru. Bulharská organizace Program svobodného přístupu k informacím[11] podala v březnu roku 2008 bulharskému Nejvyššímu správnímu soudu stížnost proti předpisu Státní agentury pro informační technologie a komunikace a ministerstva vnitra, kterým se operátorům ukládá povinnost uchovávání údajů podle směrnice 2006/24/ES. Napadaný předpis měl být v rozporu s ustanoveními bulharské ústavy a Úmluvy o ochraně lidských práv a základních svobod (dále jen EÚLP). Okruh zasažených práv byl stejný jako v případě německého, českého i rumunského podání. V prosinci roku 2008 rozhodl pětičlenný senát Nejvyššího správního soudu, že dotčené právní předpisy představují zásah do práva na ochranu soukromí a telekomunikačního tajemství a tyto zrušil. Konkrétně se jednalo o čl. 5 výše uvedeného předpisu, podle kterého mělo bulharské ministerstvo vnitra pasivní přístup ke všem uchovaným údajům prostřednictvím počítačového terminálu a bulharské informační služby a silové složky obdobný přístup využívaly bez nutnosti schválení soudem. Soud se k problému vyjádřil v tom směru, že v takových případech nebyly dány žádné záruky na ochranu ústavně zakotveného práva na soukromí, čest a důstojnost. Zajímavé je, že se soud ve svém rozhodnutí nezaobíral otázkou ochrany osobních údajů.

Svoji přednášku uzavřel Mgr. Guľaša krátkým představením posledního vývoje na poli data retention. Jak uvedl, „*k čemu se ‚neodvážil‘ německý Spolkový ústavní soud, zrealizoval irský High Court, když prohlásil, že předloží Evropskému soudnímu dvoru předběžnou otázku spojenou s posouzením platnosti data retention směrnice*“. V současné době tak irský High Court formuluje přesné znění předběžné otázky.

Hrozba plošných odposlechů

Po přednesení obou přednášek následovala diskuse s přednášejícími a zástupci z řad odborné veřejnosti. Debata se zaměřovala zejména na proporcionalitu právní úpravy data retention. K otázce vhodnosti data retention zazněly názory i pro jeho zachování. Důvodem pro existenci data retention byla zejména ekonomická stránka věci – pokud by bezpečnostní složky státu o konkrétní údaje měly opravdu zájem, jsou si je schopny stejně obstarat, ovšem s mnohonásobně vyššími náklady. Dále bylo poukázáno na fakt, že provozní údaje nutné pro vyúčtování služeb elektronických komu-

11 Access to Information Programme od roku 1996 sdružuje rumunské novináře, právníky, sociology a ekonomy za účelem propagace využívání práva na informace a podpory veřejné diskuse o vztahu lidských práv a jejich narušování využíváním nových technologií.

nikací[12] jsou operátory stejně uchovávány, a to, jak ukázala studie[13] občanského sdružení Iuridicum Remedium, po dobu delší než zákonem stanovenou. Následovala debata, nakolik by bylo možné tyto údaje využít při vyšetřování závažné trestné činnosti a zda by mohla existovat jistá „light" verze data retention. Tématem, jemuž se dále věnovala pozornost, bylo i porovnání úpravy data retention a odposlechu telekomunikačního provozu. *„Připustíme-li plošné uchovávání provozních a lokalizačních údajů, přičemž je ale zároveň postavíme co do ústavněprávní ochrany na roveň s odposlechy, budou se jen těžko hledat argumenty pro nedovolenost plošných odposlechů,"* uvedl k problematickému vztahu dovolenosti a přiměřenosti zásahu do těchto základních práv JUDr. Radim Polčák, Ph.D., vedoucí Ústavu práva a technologií a zároveň moderátor workshopu.

Čekání na rozhodnutí Evropského soudního dvora

Jak zaznělo v závěru workshopu, budoucnost právní úpravy data retention je opředena spoustou otazníků. V mnoha zemích EU je uchovávání údajů napadáno před nejvyššími orgány ochrany ústavnosti, a to povětšinou úspěšně. Klíčovým zvratem je ovšem rozhodnutí německého soudu o ústavní stížnosti, které by se dalo komprimovat do hesla *„data retention v principu ANO, nejasná právní úprava data retention NE"*. Toto „vítězství" obhájců plošného uchovávání provozních a lokalizačních údajů je ale pouze krátkodobé. Rozhodující pro osud data retention v evropském právním prostředí bude totiž rozhodnutí Evropského soudního dvora o předběžné otázce spojené s žádostí o přezkum platnosti data retention směrnice. I když výsledek řízení nelze jakkoliv předjímat, je jisté, že o problematice data retention ještě uslyšíme.[14]

12 Tyto údaje, co do rozsahu podstatně menší, se uchovávají na základě § 90 odst. 3 zákona o elektronických komunikacích.

13 Studie občanského sdružení Iuridicum Remedium „ISP: Co dělají provideři a telefonní operátoři s našimi daty?" – dostupná z: http://www.bigbrotherawards.cz/sites/default/files/Studie%20ISP_final.pdf.

14 Data retention je i tématem sekce Information Security na mezinárodní konferenci Cyberspace, která se koná na půdě Právnické fakulty Masarykovy univerzity ve dnech 26.–28. 11. 2010 v Brně. Více informací na www.cyberspace.muni.cz.