úřad
pro ochranu
osobních
údajů

informační bulletin
1 / 2004

TADY A TEĎ

V únoru Úřad zveřejnil svou Výroční zprávu za rok 2003, která je přístupná na internetu (www.uoou.cz), a v klasickém tištěném vydání ji předložil – v souladu se zákonem o ochraně osobních údajů – zákonodárcům.

Zájemcům může poskytnout ještě výtisky, které má k dispozici, stejně jako CD-ROM s přehledem zaregistrovaných správců osobních údajů.

Na tiskové konferenci 11. 3. 2004 byli novináři informováni mj. o kontrolní agendě Úřadu. Přehled je rovněž součástí tiskové zprávy dostupné na uvedené adrese webových stránek Úřadu.

V průběhu března probíhaly na Úřadě semináře, které se uskutečnily v rámci twinningového programu financovaného z prostředků Phare. Partnerem Úřadu byla i tentokrát španělská Agentura na ochranu dat. Tematicky byl projekt zaměřen na ochranu osobních údajů v oblasti policejních informačních systémů (Schengen, Europol, Eurojust) a v oblasti elektronických komunikací. Zúčastnit seminářů se měla možnost i odborná veřejnost a novináři.

V březnu se uskutečnilo na Úřadě setkání se zastupiteli MěČ Praha 7, které se vyvinulo ve velmi intenzivní a oboustranně užitečnou tříhodinovou debatu s MěÚ Prahy 7, na jejímž území Úřad sídlí. Byla navázána spolupráce, která bude pokračovat, mj. setkáním s občany a pracovníky úřadu MěČ Praha 7.

Nové kompetence Úřadu

Úřadu pro ochranu osobních údajů je svěřena **nová kompetence vyplývající z nedávno přijaté novely zákona o evidenci obyvatel** (č. 133/2000 Sb., ve znění zákona 53/2004 Sb.): Úřad bude projednávat správní delikty právnických osob a podnikajících fyzických osob za neoprávněné nakládání s rodným číslem a neoprávněné využívání rodného čísla. S účinností od 1. dubna 2004 je Úřad připraven přijímat a vyřizovat podněty týkající se porušení povinností osob při využívání rodného čísla nebo nakládání s ním. Právnické a fyzické osoby, které do dne nabytí účinnosti zákona využívaly rodná čísla v souvislosti s plněním svých úkolů a s podnikáním, jsou povinny rodná čísla z takto vedených informačních systémů, evidencí apod. odstranit do 31. prosince 2005, pokud nejde o případy uvedené v § 13 c jmenovaného zákona. V podrobnostech viz ***Stanovisko Úřadu č. 4/2004 – Aplikační výklad k části zákona č. 133/2000 Sb. o evidenci obyvatel a rodných číslech a o změně některých zákonů*** (zákon o evidenci obyvatel) v platném znění.

Nové kompetence očekává Úřad také ***v oblasti elektronických komunikací. Vyplývá to z návrhu zákona o některých službách informační společnosti***, jehož návrh předložilo Ministerstvo informatiky. Úřadu má být uložena dozorová povinnost nad dodržováním šíření obchodních sdělení v souladu se Směrnicí 2000/31/ES o elektronickém obchodu a Směrnicí 2002/58/ES o soukromí a elektronických komunikacích. Sankční postih za porušení příslušného ustanovení zákona by opravňoval Úřad uložit pokutu až do výše 10 milionů Kč.

V průběhu roku 2004 získá zřejmě Úřad ještě ***kompetence vyplývající z návrhu zákona o elektronických komunikacích***. Občan jakožto uživatel telekomunikačních nebo jiných elektronických služeb, bude-li se cítit ohrožen činností operátora nebo jiného odpovědného subjektu ve svém právu na ochranu soukromí, bude se moci v budoucnu obrátit s žádostí o nápravu stavu na Úřad pro

ochranu osobních údajů. Všechno ale bude záviset na Parlamentem přijatém znění.
Podrobný rozbor nových navrhovaných kompetencí Úřadu je zveřejněn v částce 31. úředního Věstníku a je rovněž dostupný na webových stránkách Úřadu (www.uoou.cz).

KONTROLNÍ ČINNOST ÚŘADU V 1. ČTVRTLETÍ ROKU 2004

Inspektoři Úřadu ukončili 10 kontrol, 21 kontrol probíhá, zahájeno bylo 15 kontrol.
Kontrolní odbor Úřadu přijal celkem 96 stížností, z toho je 54 případů v šetření, 15 případů bylo postoupeno inspektorům Úřadu, 4 Odboru správního rozhodování a 23 případů bylo ukončeno.
V 9 případech nabylo rozhodnutí Odboru správního rozhodování právní moci. O udílených sankcích bude Úřad informovat na svých pravidelných čtvrtletních tiskových konferencích.

Přehled stanovisek vydaných Úřadem

1. STANOVISKO č. 1/2000 – prosinec 2000 (Věstník 1/2001)
   Vedení dokumentace pacientů ve zdravotnictví
2. STANOVISKO č. 1/2001 – duben 2001 (Věstník 3/2001)
   Zveřejňování jmen dlužníků
3. STANOVISKO č. 2/2001 – říjen 2001 (Věstník 12/2001)
   Zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací
4. STANOVISKO č. 1/2002 – srpen 2002 (Věstník 19/2002)
   Zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče
5. STANOVISKO č. 2/2002 – srpen 2002 (Věstník 20/2002)
   Zpracovávání osobních údajů v souvislosti s činností knihovny
6. STANOVISKO č. 1/2004 – leden 2004 (Věstník 30/2004)
   Evidence při vstupech do budov
7. STANOVISKO č. 2/2004 – leden 2004 (Věstník 30/2004)
   Zpřístupňování a zveřejňování osobních údajů z jednání zastupitelstev a rad obcí a krajů
8. STANOVISKO č. 3/2004 – leden 2004 (Věstník 30/2004)
   Zpracování osobních údajů v souvislosti s prováděním klinického hodnocení léčiv a léčivých přípravků

Všechna stanoviska jsou v plném znění dostupná rovněž na internetových stránkách (www.uoou.cz)
.

Ochrana osobních údajů ve sdělovacích prostředcích v ČR

Ze statistiky článků, zmínek, citací apod. na výše uvedené téma, kterou zpracovalo tiskové oddělení Úřadu, vyplývá, že v uplynulém roce se jich v českých médiích objevilo zhruba 1450.
Sledovaná média přinášela zmínky o této problematice skoro každodenně, a to v rozmanitých souvislostech a v kontextu s nejrůznějšími oblastmi života naší společnosti. I média tedy mají nemalou zásluhu na tom, že povědomí veřejnosti o základních principech ochrany osobních údajů a o jejich přínosu pro zdravě fungující demokratickou společnost je stále silnější.

Poznatky a praktické zkušenosti Úřadu vypovídají o tom, že lidé i organizace si stále intenzivněji uvědomují, že ochrana osobních údajů a soukromí je v dnešní době nejenom užitečná a prospěšná, ale také nezbytná. Občané mají nyní v oblasti ochrany osobních údajů a soukromí výraznější cítění pro svá práva. Na druhé straně i úřady a další organizace učinily na tomto poli několik významných pokroků ve vnímání svých povinností.

Stále ovšem Úřad zaznamenává také reakce zcela opačné. Za obzvlášť alarmující považuje tento fakt v případech, kdy se ukazuje elementární neznalost zákonů, minimální respekt k ochraně zá-

kladních lidských práv a hluboká ignorance evropské legislativy ze strany veřejných činitelů, volených zástupců občanů (např. starostů, nebo hejtmana). Proto i mediální zájem o problematiku ochrany osobních údajů považuje Úřad za pozitivní službu občanům.

NEMĚLO BY VÁM UNIKNOUT

Řečtí ochránci dat nepovolili experiment EU – inspirace pro českou legislativu

Počátkem listopadu 2003 vzbudilo zájem evropských ochránců dat rozhodnutí Řecka nepovolit experimentální projekt EU na athénském letišti.

Oč v této věci jde?

Evropská komise se zabývá problematikou použití biometrické identifikace pasažérů s cílem nalézt tak nástroj zvyšující bezpečnost leteckého provozu. Společně se švýcarským úřadem pro vědu a vzdělávání připravila projekt "s-Travel", který by měl využívat biometriky otisku prstu a oční duhovky pro bezpečnou identifikaci leteckých pasažérů. V projektu mají být použity čipové karty a speciální čtecí a záznamové zařízení umístěné na letištích.

Projekt "s-Travel" měl být experimentálně ověřen u dobrovolníků-pasažérů, kteří cestují mezi italským Milánem a řeckým hlavním městem. Projekt používá řadu bezpečnostních prvků (např. na čipové kartě mají být biometrické údaje elektronicky podepsány a šifrovány). Používání biometrické identifikace mělo být prováděno se souhlasem pasažérů. Přesto řecký úřad pro ochranu dat (Hellenic Republic Authority for the Protection of Personal Data) nesouhlasil s prováděním experimentu na athénském letišti.

Velice zajímavé a poučné je zdůvodnění rozhodnutí řeckého úřadu (Decision no. 52/2003). Odvolává se na řecký zákon o ochraně dat z roku 1997 a uvádí, že jakékoliv zpracování dat, jež není nezbytné pro dosažení stanoveného účelu je nelegitimní. A to i přesto, že k takovému zpracování dá subjekt údajů souhlas. S odvoláním na zákon se v rozhodnutí říká, že nelegitimnímu zpracování nemůže dát „punc" legitimity souhlas subjektu údajů. Souhlas samotný nemůže umožnit jakékoliv zpracování dat, které je v rozporu se zásadou účelu a nezbytnosti. Souhlas subjektu údajů nemůže zrušit protiprávní podstatu zpracování dat. Verifikaci pasažérů lze docílit mírnějším způsobem – když cestující předloží identifikační doklad současně s letenkou a palubní vstupenkou. Navíc úřad argumentuje tím, že verifikace pasažérů využívající při odbavování cestujících biometrické údaje neřeší otázky letové bezpečnosti, nýbrž je jen organizačním zdokonalením pro letecké společnosti. S ohledem na tyto skutečnosti řecký úřad považuje zpracování biometrických údajů v projektu „s-Travel" za nelegitimní, a tedy shromažďování a zpracování biometrických údajů o pasažérech na athénském letišti nepovolil.

Rozhodnutí řeckého úřadu je pro prostředí ochrany osobních údajů v České republice velmi inspirativní, a to zejména proto, že i český úřad se neustále setkává s představou správců, že udělením souhlasu subjektu údajů se dá často zhojit skutečnost, že správce nemá pro zpracování dat potřebné právní podmínky.

Těmto představám částečně odpovídá i dosavadní znění § 5 odst. 5 věty prvé českého zákona o ochraně osobních údajů, které upravuje podmínky souhlasu se zpracováním. Proto je jistě dobré, že se již tento poněkud zavádějící text v připravované novele českého zákona nevyskytuje.

Zajímavé a poučné je také zdůvodnění rozhodnutí řeckého úřadu: Ukazuje totiž, že souhlas subjektu údajů není způsob, jakým lze legitimizovat jakékoliv zpracování osobních údajů. Souhlas může být relevantní pouze za předpokladu, že správce splní také ostatní povinnosti uložené mu zákonem o ochraně osobních údajů, včetně povinností podle § 5 zákona. Např. nebude nadále možné souhlasem subjektu údajů obhajovat nadměrné zpracování osobních údajů či zpracování, která nejsou nezbytná pro naplnění stanoveného účelu. V tomto ohledu je také upraven český zákon; současně

jsou novelizována všechna jeho ustanovení týkající se základních principů souhlasu subjektu údajů se zpracováním osobních údajů. Novela zákona prochází legislativním procesem a měla by vstoupit v platnost dnem přistoupení České republiky do Evropské unie.

Evidence při vstupech do budov

Všichni známe situaci, kdy při vstupu do budovy, kam jdeme buď na návštěvu, nebo na jednání, jsme více či méně příjemným způsobem požádání – „Zapište se mi". Je taková žádost oprávněná? Které z našich osobních údajů od nás mohou být požadovány?

V určitých případech, kdy objekt, který navštívíme, není určen k běžným návštěvám veřejnosti, má vlastník objektu právo od nás požadovat informace o naší osobě.

Rozsah údajů, který na nás může být vyžadován lze shrnout následujícím způsobem:

1. Jdeme na služební jednání – uvádíme své jméno, příjmení a předkládáme svůj služební průkaz, jehož číslo, včetně názvu vysílající instituce, lze v této souvislosti zaznamenat.
2. Jdeme na jednání, které je vyvoláno z našeho podnětu – uvádíme své jméno a příjmení a předkládáme svůj občanský průkaz nebo cestovní doklad, jehož číslo lze opět v této souvislosti zaznamenat.

Účelem poskytování těchto údajů je naše následná identifikace v případě mimořádné události v době našeho pobytu v objektu. Mimořádnou událost by zpravidla šetřila Policie ČR a pro tu by rozsah výše uváděných údajů byl dostačující, aby mohla v rámci svých kompetencí konat potřebné kroky.

V případě, že by po nás byly požadovány ještě jiné doplňující údaje jako např. adresa našeho bydliště, docházelo by již k porušování zákona o ochraně osobních údajů.

Tím, že vlastník objektu od nás získal naše osobní údaje, se stává ovšem správcem těchto údajů a jeho povinností je s těmito údaji nakládat podle zákona o ochraně osobních údajů. Je například nepřípustné, aby údaje shromážděné k tomuto účelu byly dále zpracovávány k jinému účelu, nebo aby byla překračována lhůta nezbytná k jejich uchovávání. Každý provozovatel budovy, nebo vlastník objektu, by měl podle svých možností a podle charakteru své instituce, zvážit nezbytnost a rozsah zjišťovaných osobních údajů návštěvníků objektu. Nabízí se také například možnost zřízení místnosti pro návštěvy u vstupu do objektu, nebo možnost doprovázení návštěvníků navštíveným zaměstnancem apod.

Plné znění Stanoviska Úřadu pro ochranu osobních údajů k této problematice je k dispozici ve Věstníku, částka 30/2004 a na internetových stránkách Úřadu.

Informace z jednání zastupitelstev a rady obcí a krajů

Každý z nás se určitým způsobem podílí na veřejném životě v místě, kde žije. Někdo aktivněji, jiný pouze okrajově. Většinou se začneme zajímat o správu věcí veřejných v okamžiku, kdy se nás věc začne dotýkat osobně, nebo když jsme v ní sami nějakým způsobem zaangažováni.

Častým dotazem adresovaným Úřadu je, jak postupovat při poskytování nebo naopak získávání informací ze zápisů z jednání zastupitelstva a rady a z usnesení těchto orgánů a jak je zabezpečena ochrana osobních údajů v těchto materiálech. Pro snadnější orientaci lze shrnout:

Zasedání zastupitelstva obce, hl. m. Prahy a krajů ***jsou veřejná*** a může se jich tedy zúčastnit kdokoliv. O jednání zastupitelstva obce se vyhotovuje zápis, který je podle zákona o obcích k nahlédnutí na obecním úřadě.

V Praze je zápis uložen k nahlédnutí na Magistrátu hl. m. Prahy (dle zákona o hl. městě Praze). Zápis z jednání zastupitelstva kraje je uložen k nahlédnutí u krajského úřadu (dle zákona o krajích).

Zákon o obcích, hl. m. Praze a o krajích / dále jen „zákon"/ umožňuje, že do zápisu ze zasedání výše uvedených zastupitelstev v jejich plném znění mohou občané sami zdarma nahlížet nebo si pořizovat výpisy z nich, jestliže splňují tyto podmínky:

- jsou starší 18 let věku a mají trvalý pobyt v daném místě,
- jsou vlastníky nemovitosti (stavby, byty, pozemky) na daných místech,
- jsou cizími státními příslušníky, kteří mají trvalý pobyt v těchto lokalitách.

A co ostatní? Jiné fyzické a právnické osoby mají také možnost získat informace o jednání zastupitelstva v souladu se zákonem o svobodném přístupu k informacím, ale osobní údaje, které tyto zápisy obsahují, musejí být redukovány nebo anonymizovány. V tomto případě mohou obce za poskytování informací žádat finanční úhradu.

Zasedání rady jsou neveřejná. Okruh osob, které se mohou zúčastnit je stanoven zákonem. Zápis z rady obce musí být uložen u obecního úřadu k nahlédnutí členům zastupitelstva. Jiná je situace se zápisem ze zasedání rad hl. m. Prahy a krajů, kde pro nahlížení a pořizování výpisu platí stejná zásada jako pro zápisy ze zasedání zastupitelstva.

A jak je to s ochranou osobních údajů obsažených v těchto dokumentech? Úřad dospěl k závěru, že ***tyto dokumenty jsou výsledkem systematického shromažďování osobních údajů***, a proto podléhají režimu zákona o ochraně osobních údajů. Při zveřejňování informací z jednání a usnesení zastupitelstva nebo rady na internetu, v tisku a jiných médiích, nebo při podávání informací dalším osobám ***je třeba zveřejňované osobní údaje anonymizovat***, případně rozsah zpřístupňovaných osobních údajů ve zveřejňované verzi dokumentu omezit. Úřad také doporučuje, aby byla veřejnost informována o tom, že zveřejňovaná verze je upravená.

Plné znění Stanoviska č.2/2004, které se týká uvedené problematiky, je k dispozici ve Věstníku č. 30 a na internetových stránkách Úřadu.

Účinná obrana aneb nenechte se vytočit!

Antivirové programy dnes již nabízejí účinnou ochranu před nežádoucími programy typu tzv. „dialers". Co však vlastně „dialers"jsou? Jde o programy aktivně pracující na pozadí systému osobního počítače, které se nainstalují na vaše PC, většinou bez vašeho vědomí. Pokaždé, když se připojíte k internetu, tyto programy automaticky převezmou realizaci telefonického připojení, přičemž použijí služby, která má velmi vysoké telekomunikační poplatky. Uživatel si uvědomí, že něco není v pořádku až ve chvíli, kdy obdrží fakturu za telekomunikační služby, přičemž účtovaná částka je obrovská a zcela neúměrná realizovanému telekomunikačnímu provozu. Připravovaný zákon o elektronických komunikacích by měl stanovit operátorům jak mají řešit tento problém.

Nové antivirové nástroje dokáží přítomnost těchto nežádoucích programů rozpoznat a spolehlivě je odstranit.

Více informací najdete například na velkém množství zahraničních i tuzemských internetových stránek, které se zabývají antivirovou problematikou.

TÉMA: OSOBNÍ IDENTIFIKÁTORY

Evropská unie
Osobní identifikátory: Situace v EU

Také legislativa platná v Evropské unii si je plně vědoma rizik plynoucích z tzv. křížení (propojování) databází, rizik jež existence obecných osobních identifikátorů vyvolává. Proto také Směrnice 95/46/ES Evropského Parlamentu a Rady o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů z 24. 10. 1995 v čl. 8, odst. 7 stanoví:

„Členské státy určí podmínky, za kterých může být předmětem zpracování národní identifikační číslo nebo jakýkoli jiný obecně užívaný identifikátor."

Porovnáním rychle zjistíme, že praxe týkající se osobních identifikačních čísel se v různých zemích značně odlišuje. Předkládáme zde zjednodušující shrnutí odlišností do několika tabulek.

Následující tabulka ukazuje, ve kterých zemích EU jsou zavedena osobní identifikační čísla:

Žádné osobní identifikační číslo	*Osobní identifikační číslo je zavedeno*
Spolková republika Německo	Belgie
Řecko	Dánsko
Portugalsko [1/]	Španělsko [2/]
Spojené království [3/]	Francie
	Irsko
	Itálie
	Lucembursko
	Nizozemí
	Rakousko
	Finsko
	Švédsko

Tato tabulka uvádí přehled zemí EU podle způsobu ***používání*** osobních identifikačních čísel:

Oborové číslo	*Obecné používání identifikačního čísla*
Spolková republika Německo	Belgie
Francie	Dánsko
Řecko	Finsko
Irsko [4/]	Lucembursko
Itálie	Švédsko
Nizozemí	
Rakousko	
Portugalsko	
Španělsko	
Spojené království	

[1/] Čl. 35, odst. 5 portugalské ústavy přidělování osobních identifikátorů zakazuje.
[2/] Specifikum: Ve Španělsku je identifikačním číslem číslo průkazu totožnosti .
[3/] Ve Spojeném království existuje právní základ umožňující vytvoření „identifikačního čísla", ten však dosud nebyl nijak konkretizován.
[4/] V Irsku sice od r. 1998 existuje tzv. „Public Service Number", jeho používání však není všeobecné (např. zákaz jeho používání v soukromém sektoru a úplný zákaz jeho používání policejními složkami). S jeho zavedením navíc došlo k několika dalším omezením při předávání osobních údajů.

Z tabulek vyplývá, že osobní identifikační čísla jsou sice zavedena ve dvou třetinách zemí Evropské unie, avšak pouze necelá polovina zemí z tohoto počtu jich využívá všeobecně, tedy v různých oblastech státní správy. Navíc legislativa zemí, v nichž je všeobecné užití těchto čísel zavedeno, zahrnuje klauzuli, která stanoví, že tento identifikátor může být použit pouze v případech, kdy je přesné určení totožnosti nezbytné.

Vidíme tedy, že tyto země přistoupily na zásadu, že všeobecné používání osobního identifikátoru by nemělo být rozšířeno „až příliš obecně". Identifikátor by správně měl být využíván pouze tehdy, je-li to ospravedlněno konkrétní právní nebo administrativní finalitou.

Co se týče pojetí osobních identifikátorů na mezinárodní úrovni, je dobré připomenout zde studii Rady Evropy z r. 1991, jejíž zásady jsou stále platné, zejména tyto její teze:

- Osobní identifikační čísla v souvislosti s využíváním nových informačních technologií významně přispívají růstu administrativní moci státu.
- V některých zemích (např. Francie, Nizozemí) stála právě diskuse o osobních identifikačních číslech u zrodu legislativy týkající se ochrany osobních údajů.
- Současná praxe ukazuje, že diskuse o riziku šíření a stále častějšího používání těchto identifikátorů nemá pouze teoretický charakter.

Velká Británie
Identifikační karty za £ 40

Velká Británie směřuje ke všeobecnému zavedení povinných identifikačních průkazů. Každý občan starší šestnácti let si bude muset tento doklad zakoupit, a to v ceně téměř 40 liber šterlinků. Tuto koncepci prosazuje britské ministerstvo vnitra.

Takový krok však vyvolává nemalou nevoli v prostředí občanských sdružení pro občanská práva. Právě tyto organizace totiž proti snahám o plošné zavádění jakýchkoli osobních průkazů už dlouho protestují. Je velmi pravděpodobné, že stejná bude i reakce řady voličů, kteří projeví pramalé pochopení pro to, že si budou muset zaplatit za další mocný nástroj státního dohledu.

Každá identifikační karta by měla obsahovat biometrická data – obraz oční duhovky a otisk prstu –, aby byla policii a jiným k tomu oprávněným autoritám umožněna identifikace držitele tohoto osobního dokladu.

Ačkoli držitelé průkazu nebudou povinni mít u sebe tento průkaz neustále (jako je tomu v některých zemích), po výzvě k jeho předložení by tak měli učinit v několika málo následujících dnech. Občané si také budou moci nechat zanést (samozřejmě opět po zaplacení zvláštního poplatku) výše uvedená biometrická data do svých pasů a řidičských průkazů.

Identifikační karty budou bezplatné pro důchodce ve věku nad 75 let, pro šestnáctileté osoby a dále pro osoby s nízkým příjmem. I tito občané však budou muset odevzdat státu menší poplatek ve výši 5 £. Ostatní budou muset na pokrytí příslušných nákladů přispět částkou 39 £.

Příslušná legislativa k těmto opatřením by měla vstoupit v platnost ještě v letošním roce.

Britská vláda bude vést osobní údaje občanů v ústřední počítačové databázi. I tento krok vyděsil představitele organizací, které se věnují dodržování občanských práv a svobod.

Vládní činitelé, kteří zavedení identifikačních karet prosazují, však argumentují tím, že takové opatření vychází ze silné veřejné podpory, zejména po teroristickém útoku na New York, k němuž došlo 11. září 2001, a v souvislosti s nutností energičtějšího postupu vůči teroristům vůbec. Zastánci těchto průkazů také vyvracejí argumenty, že takový krok nutně přivodí omezení občanských svobod. Tvrdí, že tyto svobody budou naopak posíleny, neboť společnost bude lépe chráněna před terorismem a organizovaným zločinem. Je zde ovšem také dobře organizovaná menšina, která je proti identifikačním kartám. Údaje obsažené v kartách však budou dostatečně omezeny, aby nemohly být různými organizacemi jakýmkoli způsobem zneužity. Přívrženci ID karet dodávají, že právo občana na ochranu soukromí nebude nijak narušeno, stejně jako není porušeno ani v jiných demokratických státech, kde je používání osobních průkazů totožnosti běžné.

Švýcarsko
Otazníky kolem osobního identifikátoru

S široce pojatým zaváděním jednotného spolkového identifikátoru osob počítá návrh nového spolkového zákona, týkajícího se harmonizace registru obyvatel s ostatními úředními registry osob. V odborných kruzích se však návrh setkává se zjevným nesouhlasem.

Spolkový úřad pro ochranu osobních údajů a švýcarští komisaři pro ochranu osobních údajů se totiž domnívají, že zavedení takového čísla k jiným než ke statistickým účelům je z hlediska ochrany osobních údajů nesmírně pochybným krokem.

Pan Giovanni Biaggini, profesor veřejného a správního práva na univerzitě v Curychu, vypracoval na jejich žádost odborný posudek, který oprávněnost jejich výhrad potvrzuje.

Text posudku profesora Biagginiho je (v německém jazyce) umístěn na internetové adrese http://www.edsb.ch/d/themen/weitere/epid/gutachten-biaggini.pdf.

Poznámka:
viz též glosa předsedy Úřadu ze dne 4. 6. 2003
(http://www.uoou.cz/aktuality.php3)

Čína oznamuje zavádění čipových karet

Čína oznámila, že v březnu 2004 "odstartuje" na světě nejrozsáhlejší program v oblasti zavádění elektronických identifikačních karet. Vláda tak přistoupí k nahrazování téměř jedné miliardy stávajících papírových národních ID karet za jejich novou čipovou verzi. Ministerstvo pro ochranu veřejnosti oznámilo, že očekává realizaci tohoto celostátního programu do konce roku 2008. Do této doby by měla být vydána celkem jedna miliarda čipových identifikačních karet.

„Duší" nového principu těchto nových karet je zabudovaný miniaturní mikročip, který uchovává osobní informace každého jednotlivce. Mikročip lze elektronicky číst a je možné jej srovnávat s databázemi, které shromažďují a uchovávají čínské tajné služby. Podle sdělení ministerského úředníka tento nový typ karty posílí schopnost vlády lépe se orientovat ve změnách a přemisťování obyvatelstva v souvislosti s možností svobodného pohybu občanů.

Nový program výměny identifikačních karet v Číně pravděpodobně vyburcuje velkou mezinárodní debatu na téma „čipové karty", které již vyvolaly odpor ochránců soukromí v USA, Velké Británii a Austrálii, zatímco evropské a asijské vlády je přijímají kladně. Mikročip byl vyvinut v Institute of Microelectonics na China's Tsinghua University a Qinghua Tongfand Microelectronics Co., která je dceřinou společností zmíněné university a je jí také kontrolována.

Zdroj : Dow Jones Neswire, January 27, 2004,
http://online.wsj.com China Prepaes to Introduce „smart" Identification Cards,
http://online.wsj.com/article/ o,,SB 107525820440013805,00.html

Biometrie a osobní doklady: identifikace nebo verifikace?

V souvislosti se současným dynamickým rozvojem oboru biometrie se dnes často hovoří o nové generaci identifikačních průkazů a dalších dokladů. Nyní jde o to, jak při zachování základního smyslu a účelu takových dokumentů zachovat také respektování zásad ochrany osobních údajů jednotlivců.

Nové cestovní doklady by kromě digitální fotografie měly obsahovat také digitální otisk prstu nebo digitálně zpracovaný obraz oční duhovky (ten je rovněž, stejně jako otisk prstu, u každého člověka jedinečný). Zavádění takových dokumentů však provázejí velmi živé diskuse a polemiky, a to nejenom mezi odborníky, ale také v řadách politiků i v široké veřejnosti. Tak například ministerstvo vnitra Velké Británie v poslední době prosazuje postupné zavádění biometrických průkazů totožnosti, přičemž v zájmu realizace této představy zahájilo masivní mediální kampaň. Je však třeba říci, že mezi britskými občany (ani v samotné britské vládě) se tato idea prozatím netěší všeobecnému konsensu. Není divu: vždyť v Británii dosud nejsou zavedeny ani klasické „občanské průkazy", které jsou v kontinentální části Evropy běžnou záležitostí. Ministr Blunkett byl dokonce za svou koncepci osočen z „totalitářských" tendencí. A to ponecháváme stranou skutečnost, že podle názoru některých odborníků biometrické identifikační metody nejsou dosud po technické stránce zcela spolehlivé.

Na druhé straně oceánu, v USA, si tolik starostí nedělají: novou generaci cestovních dokladů s biometrickými údaji chtějí zavést již letos a od roku 2006 plánují vyžadovat podobné doklady od ostatních zemí. Nebude-li tato podmínka některou zemí splněna, bude jí ze strany USA hrozit zavedení vízové povinnosti. Ani Evropská unie v podobných projektech nezaostává: o cestovních dokladech obsahujících biometrické údaje se v létě roku 2002 hovořilo na summitu v Soluni.

Vraťme se však k titulku tohoto článku. Důležité pojmy představují v tomto kontextu výrazy „identifikace" (někdy označovaná také jako metoda „One-To-Many") a „verifikace" (někdy též „autentikace", „autentifikace", nebo metoda „One-To-One"). Identifikace je postup, při němž je sejmutý biometrický vzorek porovnáván s referenčními šablonami uloženými v příslušném seznamu a následně je zjišťováno, která referenční šablona (je-li v seznamu obsažena) danému vzorku odpovídá. Biometrický systém je schopen rozpoznat totožnost uživatele bez nutnosti jejího předchozího zadání.

Naproti tomu verifikace spočívá v postupu komparace sejmutého biometrického vzorku s jednou referenční šablonou uživatele, jehož totožnost byla zadána. Tento postup pak vede k zjištění, zda sejmutý vzorek této totožnosti odpovídá.

Podle předsedy Úřadu pro ochranu osobních údajů K. Neuwirta jsou zde oprávněné důvody k obavám, aby během vydávání nových dokladů nevznikaly „stínové" databáze o jejich držitelích. Proto také chce Úřad prosazovat takovou koncepci, při níž by biometrie sloužila zejména pro účely verifikace (tedy např. pro porovnání otisku prstu na mikročipu v pase se skutečným otiskem prstu pasažéra) a nikoli pro účely identifikace (plné ověření totožnosti cestujícího porovnáním s údaji v ústřední databázi).

Se zaváděním těchto nových metod zjišťování totožnosti se tak vrací jeden starý problém: Tábor argumentující pro „tvrdší linii", tedy pro razantnější zásah do práv občanů na ochranu jejich osobních údajů a soukromí, poukazuje na větší ohrožení bezpečnosti, které zřejmě bude v průběhu 21. století běžnou realitou. Na druhou misku vah je však třeba klást důsledné respektování všech práv občanů a předcházení hrozbě totalitarismů nejrůznějších barev. Takovému nebezpečí může zavádění silných prvků kontroly občanů napomáhat. Kromě možnosti politického zneužití občanských svobod jsou zde samozřejmě nemalá rizika zneužívání kriminálního charakteru. Mezi oběma typy argumentů, z nichž každý má svá opodstatnění, bude třeba neustále nacházet rozumnou rovnováhu.

K věci: Pohled odjinud

Krádež identity

Ochrana soukromí a prosazování práva jsou mnohdy vnímány jako protikladné kategorie: Přinejmenším je jejich vztah pokládán za značně složitý. Problematika související s krádežemi identity však může vést i k jejich smíření. Krádež identity a podvody, které jsou s ní spojeny, jsou vážnou hrozbou a její negativní důsledky a dopady jsou jen stěží odhadnutelné.

To, že krádeže identity jsou předmětem zájmu policejních složek, je samozřejmé. Týkají se však také činnosti ochránců soukromí: Neboť sotva si lze představit závažnější a ofenzivnější narušení práv druhého na jeho soukromí, než situaci, kdy někdo – tím, že se neoprávněně zmocní vašich osobních údajů – předstírá, že je vámi. Všechny možné ústrky, pocity frustrace, ponížení a nedůstojnosti, jsou běžným následkem nikoli pouze samotného faktu zneužití vaší totožnosti, ale také následných a často svízelných pokusů přesvědčit úřady, se kterými musíte jednat, že jste skutečně tím, za koho se prohlašujete, a že vaše totožnost byla prostě odcizena. A všudypřítomnost a rychlost elektronického předávání dat tuto zkušenost ještě zhoršuje. Problém krádeží identity je často citován v souvislosti s prosazováním identifikačních a autentifikačních (verifikačních) metod, zejména biometrických.

Účinnost jednoduchých řešení je však iluzorní. Vyvážený přístup k této problematice bude vyžadovat její pečlivý rozbor; jinak bude mít léčba horší následky než samotná nemoc. Je známo, že například lidé v Austrálii mají silnou averzi k všeobecným osobním průkazům. Povinné jednotné osobní identifikační kódy by jistě usnadnily kontrolu shody dat. Ale jak policejní složky a ochránci soukromí sami uznávají, jestliže je určitý osobní průkaz pokládán za „důkaz" něčí totožnosti, právě tentýž průkaz se může stát snadnou a zranitelnou kořistí pro zloděje, podvodníka či nebezpečného manipulátora. Přiměřená verifikace osobní totožnosti bude vyžadovat zvážení všech eventualit tohoto problému, a to jak ze strany zákonodárců, tak z hlediska ochránců soukromí.

Paul Chadwick
Privacy Aware Vol. 1 No. 6/2003, Victoria, Austrálie

Poznámka:
Ochraně před krádeží identity se věnoval také článek „Krádež identity a jak jí předcházet", který vyšel v Bulletinu č. 1/2003.

úřad pro ochranu osobních údajů

CO NOVÉHO V ZAHRANIČÍ

Velká Británie
Britský kodex o monitorování zaměstnanců v zaměstnání

Britainęs Information Commission předložila třetí část kodexu Employment Practices Data Protection Code, kterým se opravňuje monitorování v zaměstnání. Účelem Kodexu je pomoci zaměstnavatelům plně chápat rozsah své zodpovědnosti ve chvíli, kdy tento kodex o monitorování zaměstnanců bude zaveden do praxe. Vydaná směrnice představuje třístupňový program pro zaměstnavatele. Jedním ze základních požadavků, který je kladen na zaměstnavatele shromažďující informace o zaměstnancích na počítači nebo v jiném sofistickém systému třídění, je povinnost ohlásit dozorovému orgánu (Information Commissioner) své aktivity v oblasti zpracování těchto dat. Opomenutí nebo porušení jakékoliv části zákona na ochranu dat může vést až k právním sankcím, pokutám a obžalobám. Základním smyslem vydání kodexu je snaha uvést do souladu práva zaměstnanců s dobře fungujícím chodem podniku.

Kodex zřetelně stanovuje základní požadavek kladený na zaměstnavatele – naprosto jasně pochopit účel jakéhokoliv monitorování svých zaměstnanců a také uspokojivě zabezpečit, aby konkrétní opatření byla právně zakotvena dříve, než vejdou v platnost. Velký důraz je kladen na to, aby zaměstnavatel svým zaměstnancům jasně a správně vysvětlil oprávnění zavádění monitorování. Zaměstnanci musí být vždy osloveni tak, aby si plně uvědomovali podstatu a rozsah monitorování. Pouze ojediněle a za výjimečných okolností může nastat situace, že podstata monitorování je utajena.

Neexistuje žádný právní požadavek pro zaměstnance, aby vyjádřil svůj souhlas s monitorováním, pokud monitorování bylo právoplatně ustaveno. Způsob monitorování zaměstnanců je závažná skutečnost, které je potřeba věnovat prvořadou pozornost. Zaměstnavatelé musí jasně zvážit výhody svého počínání oproti jakémukoliv nepříznivému dopadu na denní chod společnosti a uspokojivě zvládnout právní požadavky na správné zacházení se zaměstnanci. Pronikání do soukromí zaměstnanců bude oprávněné jedině v případě, že podnikatelským aktivitám zaměstnavatele by mohlo ze strany zaměstnance hrozit vážné poškození.

Zdroj: Mondaq, January 21, 2004

USA
Letecké společnosti pracují na vytvoření Jednotných zásad ochrany a odhalování soukromých údajů

Přední letecké společnosti USA se urychleně snaží vytvořit zásady odhalování údajů, aby zákazníci byli informování o tom, že společnosti mohou sdílet jejich osobní data s federální vládou. Jejich snaha je reakcí na dvě vysoce medializované kauzy, ve kterých letecké společnosti předaly vládě osobní údaje o cestujících. Letecké společnosti nyní velice pružně pracují na tom, aby své pasažéry varovaly a samy sebe tak chránily před zodpovědností, protože vláda USA nutí dopravce uspořádat údaje o pasažérech tak, aby uspořádání údajů odpovídalo programu CAPPS II. Letecké společnosti jsou pod tlakem kvůli odhalení, že Northwest Airlines opomenula informovat zákazníky o tom, že dala vládě záznamy o milionech cestujících pro tajný bezpečnostní projekt. V září společnost JetBlue přiznala, že také předala záznamy do jiného projektu.

Cestující podávají žádosti o zahájení soudního řízení s oběma leteckými společnostmi, soukromníci si stěžují na vládní úřady a členové Kongresu posílají dopisy s ostře formulovanými dotazy leteckým společnostem i vládním úřadům zahrnutým do tohoto projektu. Představitelé leteckých společností se setkali ve Washingtonu, aby projednali možnost přijetí zásad pro ochranu soukromí v takové podobě, aby bylo možné spolupracovat s programem CAPPS II. Letečtí přepravci doufají,

že se vyjasní postupy, které umožní dopravcům reorganizovat své záznamy tak, aby při plném zabezpečení soukromí zákazníků se současně limitovala i odpovědnost aerolinií. Vyjádření právníků zní: Neexistuje žádný zákon, který by zabraňoval společnostem sdílet informace mezi sebou nebo s vládou. Na druhé straně však společnosti, které nezveřejní za jakých okolností a komu informace předaly, mohou čelit žalobám ze strany zákazníků pro klamání a porušení soukromí a také vyšetřováním i pokutám ze stran státních úřadů.

Zdroj :The Wahington Post, January 24,2004, http://www.washingtonpost.com
Airlines Hustling On Data Disclosure Policies Being Drafted Undred Pressure

Evropská unie
Ochrana při předávání osobních údajů cestujících v letecké dopravě

Celý svět se v současné době snaží nalézt řešení a metody pro boj s terorismem. Jednotlivé státy v rámci zajištění bezpečnosti občanů přijímají řadu opatření. Tato problematika však přesahuje hranice států a jedině konstruktivní spolupráce a ochota dohodnout se mohou v této oblasti zaručit naději na úspěch.

V důsledku událostí z 11. září 2001 Spojené státy přijaly řadu zákonů a nařízení, požadujících po leteckých společnostech, které létají na jejich území, aby americkým úřadům předávaly osobní údaje týkající se cestujících a členů posádek přilétajících do této země nebo z ní odlétajících. Letecké společnosti, které těmto požadavkům nevyhoví, mohou čelit vysokým pokutám a dokonce ztrátě přistávacích práv, nebo po příletu do USA mohou vystavovat své pasažéry zdržení.

Předávání dat americkým úřadům vzbuzuje veřejné obavy, a kromě širokého a citlivého dopadu má také mezinárodní rozměr. Veřejnost je oprávněně znepokojena možným zneužitím propojených informačních databází, nebo nejasnostmi i omyly, ke kterým by mohlo docházet. Pro ilustraci lze uvést případ, kdy na poslední chvíli byly některé lety ze zemí EU do USA zrušeny. Důvodem byl omyl v porovnávání databáze údajů o cestujících se seznamy hledaných osob podezřelých z terorismu. Množství a citlivosti údajů, o které jde a počet cestujících dotčených tímto požadavkem Spojených států, jednalo by se asi 10 –11 milionů jednotlivců ročně, podtrhuje potřebu opatrného přístupu. Nesmí se také zapomenout na možnosti, které se tím otevírají pro „dolování dat" tzv."data mining", postihující zejména obyvatele Evropy, a na riziko všeobecného dohledu a kontroly třetím státem.

Pracovní skupina 87 Evropského parlamentu, která pracuje jako nezávislý evropský poradní orgán pro ochranu osobních dat a soukromí, vydala k otázce ochrany osobních údajů obsažených v záznamech cestujících leteckou dopravou, které mají být předávány do USA již několik stanovisek. Jde o problematiku, která se jistě bude dotýkat také mnoha našich občanů. Chceme vám proto touto cestou přiblížit poslední stanovisko pracovní skupiny a napomoci vám tak lépe se v této otázce orientovat.

Pracovní skupina ve svém stanovisku zdůrazňuje nezbytnost vytvoření ***jasného právního rámce*** pro převod údajů z leteckých společností do Spojených států takovým způsobem, který bude kompatabilní se zásadami o ochraně údajů. Spojené státy by měly poskytnout také reciprocitu a zajistit „řádný postup" pro obyvatele zemí EU. Účely předávání dat by měly být omezeny na ***boj proti teroristickým akcím*** a na kriminalitu související s terorismem. ***Seznam datových prvků by měl být přiměřený a doba uchovávání těchto údajů krátká*** a úměrná. Proces porovnávání údajů s podezřelými osobami by měl být prováděn podle vysoce kvalitních standardů s maximální možností ***zabránit omylům***. V tomto ohledu by mělo být vzato na vědomí, že si ***lze si představit i jiná řešení***, která lépe respektují zásady pro ochranu údajů, a přesto jsou však účinná. Je to například systém užívaný v Austrálii v oblasti boje proti kriminalitě.

Citlivé údaje, odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, členství v odborech a údaje týkající se zdraví nebo sexuálního života, ***by se neměly předávat***. Důležitým bodem stanoviska je také vyjádření, že údaje o cestujících by rozhodně ***neměly být využívány pro zavádění a/nebo testování systému CAPPS II*** nebo podobných systémů,

protože tyto systémy se kvalitativně odlišují od pouhého předávání údajů a vyvolávají dalekosáhlé otázky, které by měly být ještě vyjasněny. Pro vysvětlení – CAPPS II je projekt kontroly cestujících v letecké dopravě v USA, který v samotných Spojených státech je chápán jako kontroverzní a ne všemi podporovaný.

Cestujícím by měly být poskytnuty jasné, včasné a komplexní informace o tom, za jakým účelem a komu jsou jejich osobní data předávána a měla by existovat dostatečná záruka, že budou mít přístup k opravdu nezávislému mechanismu vyřizování stížností.

Závazky Spojených států by měly být ***pro americkou stranu plně právně závazné*** a také by měla být vyjasněna působnost, právní základ a význam možné ***„jednoduché mezinárodní dohody"***.

Stanovisko klade důraz na požadavek, aby ***další předávání údajů*** jiným státním nebo zahraničním orgánům bylo ***striktně omezeno***.

Letecké společnosti navrhují, aby se ***pro předávání údajů použilo metody „push"***, která by zaručovala leteckým společnostem, že by samy vybíraly a převáděly údaje úřadům ve Spojených státech. Tato metoda by tedy, na rozdíl od metody „pull", neumožňovala americkým úřadům přímý přístup do databáze leteckých společností a rezervačních systémů.

Boj proti terorismu je nezbytný, ale i v této oblasti musí být zachováván respekt k základním právům a svobodám jednotlivců, včetně práva na soukromí a ochranu osobních dat. Jak z výše uvedeného vyplývá, je tato myšlenka ve Stanovisku 2/2004 Pracovní skupiny 87 Evropského parlamentu jasně a konkrétně vyjádřena.

(Poznámka: Evropský parlament se na svém zasedání 31 .3. 2004 postavil proti dohodě, kterou Evropské komise uzavřela se Spojenými státy o poskytování údajů o cestujících na leteckých linkách z Evropy do USA. Poslanci podpořili rezoluci výboru pro lidská práva, odsuzující prozatímní dohodu s USA jako příliš vágní a nezaručující dostatečnou úroveň ochrany dat.)

Zdroj : Stanovisko 2/2004 Pracovní skupiny 87 Evropského parlamentu k odpovídající ochraně osobních údajů obsažených v záznamech PNR cestujících leteckou dopravou, která mají být předávána Úřadu cel a ochrany hranic Spojených států . Přijato dne 29.ledna 2004.

Společný orgán dozoru pro Europol: Zpráva o činnosti

23. října 2003 Společný orgán dozoru pro Europol předložil veřejnosti první zprávu o své činnosti.

Společný orgán dozoru pro Europol (Europol Joint Supervisory Body) je nezávislým orgánem, jehož členy jsou představitelé ochránců osobních údajů z 15 členských zemí Evropské unie, které ratifikovaly a přijaly Úmluvu o Europolu z roku 2003. Jeho hlavním úkolem je sledování aktivit Evropského policejního úřadu – Europolu, s cílem zabezpečit, aby činnost spočívající v ukládání, archivaci, zpracování a používání osobních údajů, jimiž tento úřad disponuje, nenarušovala práva jednotlivců. Zpráva podává v uceleném přehledu informace o činnosti Společného orgánu dozoru pro Europol za první čtyři roky jeho existence. Jejím cílem je, kromě jiného, zvýšit všeobecnou informovanost veřejnosti o působnosti a hlavních aktivitách této instituce a v povědomí veřejnosti tak posílit představu o smyslu a významu její práce.

Společný orgán dozoru pro Europol spolupracoval s Europolem např. na návrzích smluv s třetími stranami (státy, organizacemi), týkajících se přenosu osobních údajů. Pro zvýšení efektivnosti svých aktivit vypracoval Společný orgán dozoru pro Europol různé metody dozorové činnosti a zavedl systém pravidelných auditů ústředí Europolu a jeho systémů pro zpracování dat.

Společný orgán dozoru pro Europol také připravuje vlastní internetovou stránku, kde budou spolu s dalšími důležitými informacemi a dokumenty zveřejňovány (jednou za dva roky) souhrnné zprávy o jeho činnosti.

úřad pro ochranu osobních údajů

KDYŽ SE ŘEKNE...

EUROPOL – co je dobré vědět

Evropský policejní úřad Europol založilo 15 členských států Evropské unie, aby se zvýšila bezpečnost v rámci evropského prostoru. Europol je mezivládním policejním úřadem a jedním z jeho hlavních cílů je usnadnit výměnu informací mezi policiemi jednotlivých členských států. Sídlem Europolu je nizozemský Haag.

Myšlenka zřídit Evropský policejní úřad byla poprvé zmíněna na zasedání Evropské rady v Lucemburku 28. a 29. června 1991. Plán předpokládal zřízení nového orgánu, který by poskytl strukturu pro rozvíjení policejní spolupráce mezi členskými státy v oblasti prevence a boje proti vážným formám mezinárodního organizovaného zločinu, včetně terorismu a pašování drog. Úmluva zakládající Europol byla podepsána v červenci 1995 a vstoupila v platnost 1. října 1998.

Aby se zbytečně neztrácel čas čekáním na vytváření struktur policejní spolupráce definovaných v hlavě VI ***Smlouvy o Evropské unii***, byla v roce 1995 zřízena dočasná ***Protidrogová jednotka*** Europolu. Hlavním cílem této jednotky byl boj proti pašování drog a s ním spojenému praní špinavých peněz. Její kompetence byly následně rozšířeny na boj proti:

- pašování radioaktivních látek a nukleárních substancí,
- tajným přistěhovaleckým sítím,
- pašování automobilů,
- obchodu s lidskými bytostmi,
- praní špinavých peněz, spojeným se všemi výše uvedenými kriminálními aktivitami.

Europol, který převzal aktivity protidrogové jednotky, začal fungovat od 1. července 1999. Tato organizace má v současné době rovněž pravomoci k boji proti terorismu a padělání peněz.

Důležitým mezníkem v činnosti Europolu je Amsterodamská smlouva (ze dne 2. 10. 1997), která mu uděluje řadu dalších úkolů:

- koordinace a implementace určitých vyšetřování prováděných orgány členských států,
- vývoj specializovaných expertíz, které by pomohly členským státům v jejich boji s organizovaným zločinem,
- rozvoj kontaktů se státními zástupci a s vyšetřovateli, kteří se specializují na boj proti organizovanému zločinu.

Europol disponuje rozsáhlým počítačovým informačním systémem TECS (The Europol Computer System). TECS má tři základní složky: analytický systém, indexační systém (ten je již nyní dobudován) a informační systém, který je v současné době v testovací fázi. Přístup do systému je plánován pro všechny národní jazyky členských států EU.

Organizační struktura Europolu je upravena v čl. 27 a následujících Úmluvy o založení Europolu ze dne 18. 7. 1995.

Europol je odpovědný ***Radě ministrů***, která má na starosti kontrolu a řízení funkcí Europolu. Rada ministrů jmenuje ředitele Europolu a jeho zástupce a přijímá rozpočet.

Dalším orgánem Europolu je jeho ***Řídící rada***, ve které má každý členský stát jednoho zástupce s jedním hlasem. Tento orgán se schází minimálně dvakrát za rok a jeho úkolem je dohlížet na činnost Europolu.

V čele Europolu stojí jeho ***ředitel***, který je jmenován na pět let Radou ministrů. Je zodpovědný za běžný každodenní chod Europolu a zastupuje jej navenek.

Europol má působnost a uplatňuje své kompetence v 15 státech Evropské unie: Belgie, Dánsko, Finsko, Francie, Irsko, Itálie, Lucembursko, Německo, Nizozemí, Portugalsko Rakousko, Řecko, Spojené království, Španělsko, Švédsko.

Dne 5. března 2002 podepsali v Praze ministr vnitra ČR Stanislav Gross a ředitel Europolu Jürgen Storbeck ***Smlouvu o spolupráci v boji proti závažné mezinárodní trestné činnosti***. Tato smlouva poskytuje dostatečný právní základ pro budoucí spolupráci, zejména v oblasti výměny informací o konkrétních případech trestné činnosti. Velká část smlouvy je věnována také ***ochraně předávaných osobních údajů***. Smlouva se dále zaměřuje na výměnu odborných zkušeností, informací o vyšetřovacích metodách, o prevenci kriminality, o výcviku a na pomoc při vyšetřování konkrétních případů. Na základě smlouvy se předpokládá vyslání českého styčného úředníka do sídla Europolu, případně styčného úředníka Europolu do České republiky.

V současné době Evropská unie pracuje na zřízení ***společného mezinárodního policejního sboru***, který bude alespoň částečně uniformovaný a bude plnit obecné úkoly policie.

Internetové stránky Europolu jsou na adrese: www.europol.eu.int

OSOBNÍ ÚDAJE V ŠIRŠÍCH SOUVISLOSTECH

Přirozené napětí

„Víte, ve věku, kdy informace o jednotlivcích lze jednoduše najít, jednoduše prodat i jednoduše zneužít, musí vláda jednat tak, aby soukromí jednotlivců chránila." – US President G.W. Bush, při podpisu Fair and Accurate Credit Transactions Act, 4/12/03

„ Naše vláda musí mít k dispozici ty nejlepší možné informace, které použijeme tak, abychom si mohli být jisti, že praví lidé budou na správných místech, aby chránili všechny naše občany." – US President G.W. Bush, při oznámení vzniku Terrorist Threat Integration Center, mohutného projektu srovnávání dat, který propojuje informace shromažďované tajnými službami USA.

Výše uvedené výroky jsou příkladem přirozeného napětí, které zažívají zvolené vlády ve věci ochrany soukromí. Několik článků v tomto vydání Privacy Aware objasňuje toto téma. Vlády, které uznávají důležitost ochrany soukromí, vytvářejí zákony o nakládání s osobními informacemi ve státní správě i komerčním sektoru. Zákony mají možnost být konkrétní v určitých informacích o omezení shromažďování, jako například US status k zapůjčování videozáznamů jednotlivců a údajů o řidičských průkazech. Nebo zákony mohou být zevrubné, se stanovením obecných principů, které lze aplikovat na všechny typy informací v mnoha rozmanitých úpravách (zatím je takový přístup evropský a australský).

Jestliže informace znamenají moc, pak je kontrola nad informacemi tak důležitá ve vládních postupech, že zákony, které přikládají informačním tokům vynutitelná práva a povinnosti mohou být považovány vládou za překážku a iritizující prvek. Děje se tak především tehdy, když zákony o ochraně soukromí jsou něčím novým a vyžadují tak neobvyklé úpravy a vysvětlení. V takovém případě se může zdát jednodušší odporovat, blokovat postup, nebo se „problému" zbavit .

Některé vlády tomuto podléhají. Jiné ne, protože jsou možná schopny si připustit, že všichni, kteří nyní jsou „ uvnitř", tj. ve vládě, budou jednoho dne lidmi „venku" – tj. nikoli vládními činiteli. Zákony na ochranu soukromí mají naději na úspěch tam, kde je vlády akceptují jako zdroj přirozeného, nepřetržitého, avšak konstruktivního napětí.

Paul Chadwick
Victorian Privacy Commissioner
Zdroj : Privacy Aware, Vol 2 No 4 Summer 2003–04

úřad
pro ochranu
osobních
údajů

Na poslední chvíli

Dne 16. března 2004 se definitivně uzavřel spor vedený Českým statistickým úřadem proti Úřadu pro ochranu osobních údajů.

Ústavní soud odmítl stížnost Českého statistického úřadu vůči usnesení Městského soudu v Praze, který již v roce 2001 shledal neoprávněnost podání ČSÚ proti rozhodnutí předsedy Úřadu pro ochranu osobních údajů ve věci sčítání lidu, domů a bytů v roce 2000.

Proti tomuto usnesení Ústavního soudu není odvolání.

Ústavní soud již v této souvislosti jednal, když 16. 2. 2002 odmítl návrh ČSÚ na zahájení řízení v kompetenčním sporu s Úřadem pro ochranu osobních údajů.

Rekapitulace právní pozici, kterou Úřad pro ochranu osobních údajů v dané věci zaujal a důsledně zastával:

Sdělení předsedkyně Českého statistického úřadu doc. Ing. Marie Bohaté, CSc. v kontextu tiskové konference k výsledkům sčítání lidu, domů a bytů, která se konala 16.7. 2002, zejména interpretované některými novináři, uvedlo veřejnost ve zřejmý omyl.

Úřad pro ochranu osobních údajů v souladu s povinností, kterou mu ukládá zákon, konstatoval, že ČSÚ je oprávněn a povinen dle zákona o ochraně osobních údajů zpracovávat osobní údaje v souladu se zvláštním zákonem č. 158/1999 Sb., který v § 5 odst. 1 písm. a) stanoví, jaké údaje se při sčítání zjišťují o fyzických osobách. Úřad detekoval ve sčítacích arších ty údaje, jejichž sběr není v uvedeném paragrafu zákona č. 158/1999 Sb. o sčítání obyvatel, domů a bytů uveden.

Není zřejmé, proč na zahrnutí těchto údajů do taxativního vymezení statistici v době vzniku zákona č. 158/1999 Sb. netrvali už v roce 1999. Zvláštní podiv to vyvolává ve světle skutečnosti, že dne 16. 7. 2002 deklarovala předsedkyně ČSÚ údaj o počtu dětí z posledního manželství za zjišťovaný od roku 1930 a velmi důležitý pro uplatňování dobře cílené jak populační, tak imigrační politiky. K posouzení tohoto faktu jsou zajisté kompetentní demografové.

Úřad pro ochranu osobních údajů ve svém postoji a krocích ovšem vycházel ze svých kompetencí. Z těch vyplývá, že musí dbát v oblasti ochrany osobních údajů na dodržování zákona a nemůže připustit prolamování právního řádu, má-li dostát povinnostem, které mu jsou uloženy. Je třeba vidět, že nerespektování právního řádu, kterého se de facto domáhá ČSÚ v souvislosti se dvěma inkriminovanými shromážděnými údaji, by založilo mj. precedens libovolného a příležitosti vyhovujícího, účelového výkladu zákona.

Úřad pro ochranu osobních údajů je znepokojen výroky některých novinářů a faktem, že po zkušenostech, kterými prošla populace teritoria České republiky za posledního půl století, je ještě natolik ležérní postoj k zákonu možný. Jako by volání veřejnosti i novinářů po potřebě vytvořit pro demokracii v České republice efektivně fungující právní prostředí umlklo při velmi konkrétní situaci aplikování zákona, jakou například sčítání lidu, domů a bytů představuje.

Na okraj tvrzení o rozhodování soudních instancí ve sporu ČSÚ vedeného proti Úřadu pro ochranu osobních údajů uvádíme sdělení, která již Úřad dal médiím k dispozici:

Sdělení pro tisk
Úřad pro ochranu osobních údajů 22. 11. 2001:

Soudní spor, v němž se Český statistický úřad dožadoval žalobou přezkumu rozhodnutí předsedy Úřadu pro ochranu osobních údajů ve věci nakládání s některými osobními údaji při zpracování dat sčítání lidu, domů a bytů z roku 2001, zastavil Městský soud v Praze bez dalších opravných prostředků. Soud při zastavení řízení vyslovil právní názor, že stát je ve veřejnoprávních vztazích z práva žalovat u správního soudu vyloučen.

Napadená rozhodnutí předsedy ÚOOÚ jsou tak pravomocná a vykonatelná a Český statistický úřad je povinen se jimi řídit.

Dne 6.3. 2002 informoval Úřad pro ochranu osobních údajů na své tiskové konferenci o Usnesení

Ústavního soudu ze dne 16. ledna 2002, jímž soudce zpravodaj JUDr. Vlastimil Ševčík odmítl stížnost Českého statistického úřadu a shledal návrh ČSÚ jako nepřípustný.

Toto Usnesení Ústavního soudu v plném znění vyšlo v částce 19 Věstníku Úřadu pro ochranu osobních údajů.

Dne 8. 4. 2004 byla Poslaneckou sněmovnou Parlamentu přijata novela zákona o ochraně osobních údajů. Tato „euronovela" zákona zohledňuje nároky občanů zemí Evropského společenství na ochranu soukromí a plně harmonizuje český zákon o ochraně osobních údajů s příslušnou legislativou Evropské unie.

Účinnost zákona je předpokládána dnem vstupu smlouvy o přistoupení České republiky k Evropské unii v platnost, s výjimkou novelizovaných ustanovení týkajících se oprávnění Úřadu pro ochranu osobních údajů pro ukládání sankcí, která by měla nabýt účinnosti v souladu se změnami obecné právní úpravy v oblasti správního trestání dnem 1. ledna 2005.

Trestný čin: odboj právu

Zákon o ochraně osobních údajů, pokud bychom měli věřit některým výrokům, často též denního tisku, zabraňuje téměř všemu. Čestné místo v tomto výčtu ovšem nepochybně zaujímá problematika doručování a výkonu nejrůznějších rozhodnutí.

V 16. století však v Čechách žádný zákon o ochraně osobních údajů neexistoval a vše tedy zřejmě běželo zcela hladce.

Tehdejší vítěz sporu si proto zpravidla u zemských desek nejprve vyžádal „list na zvod". Na jeho základě se pak povinný měl dostavit k příslušným úředníkům a ti provedli formální převod vlastnictví. Pokud ale dlužník nereagoval, byl vydán tzv. obranní list, autorizovaný nejvyšším purkrabím. Ten zároveň určil svého zřízence nazývaného „zemský holomek", který dokument doručil a na příslušném statku představil nového pána.

Doručování písemností té doby také mělo své zvláštnosti. Samozřejmě netřeba zdůrazňovat fakt neexistence dnes běžné pošty i složitosti cestování.

Pro nás jsou důležitější formální pravidla. Byla velmi podrobná. Posel kupříkladu nesměl být ozbrojen a musel se vykázat velkou pečetí zemského soudu s vyobrazením svatého Václava. K předání dokumentu muselo dojít ve všední den, a to ještě dopoledne.

Naproti tomu však osoba doručitele byla považována za nedotknutelnou. Každé násilí proti ní se tudíž považovalo za trestný čin odboje právu. Takový šestnácté století stíhalo smrtí a konfiskací majetku.

Pojďme ale již k přímo k věci.

Nedlouho po svatém Valentinovi léta páně 1526 se na Český Krumlov s obranním listem dostavil Tomáš Šilhavý, přísežný holomek úřadu nejvyššího purkrabství pražského spolu s doprovodem. Po chvilce čekání se příchozích ujal další purkrabí, tentokrát ovšem krumlovský. Nezavedl je však tam kam měl, tedy k místnímu vladaři Jindřichovi z Rožmberka, nýbrž rovnou do věže. Zde se nacházelo vězení v podobě hladomorny v níž nebozí státní úředníci bez jakéhokoli vysvětlení zůstali až do dalšího rána.

Teprve tehdy s nimi kdosi začal „komunikovat". Byli to pověžní, další podřízení krumlovského pána. Navázaný kontakt ovšem byl poněkud jednostranný. Spočíval pouze v konstatacích, že zadržovaní jsou podvodníci, vykazují se falešnými doklady a mají se tedy co těšit na odpoledne.

A pověžní opravdu nelhali.

Zpočátku to ale nijak špatně nevypadalo. Nejprve se k zadrženým dostavil sám pan Jindřich z Rožmberka. Z jámy nechal vytáhnout Tomáše Šilhavého a konečně od něj převzal do-

ručované písemnosti.

Na žádné pečlivé pročtení, jak by se dalo očekávat, už ale nedošlo. Krumlovský pán totiž listiny i s pečetěmi vzápětí rozřezal na několik kusů. Na to užaslého posla vyzval k jejich konzumaci. Ten sice okamžik váhal, hrozící kyj v rukou Jindřicha z Rožmberka ovšem představoval velmi obtížně vyvratitelný argument.

Tomáš se ale možná nechal uchlácholit i faktem, že na něj připadla pouze spravedlivá část právě naporcovaných dokumentů. Dostalo se mu jen jediné výsady – osobně měl sníst vyobrazení svatého Václava.

Vězněné poselstvo se postupně pustilo do jakési nedobrovolné odpolední svačiny a Jindřich z Rožmberka proto mohl být spokojen. Všem jedlíkům dokonce poručil k zapití přinést sklenici dobrého vína. Pak ještě Tomáši sdělil, že šilhá jako pán z Pernštejna (vidíme jak naše příjmení mají mnohdy reálný základ) a celou delegaci za doprovodu ohařů i dalších ponaučení vykázal se zámku.

Tím náš příběh vlastně již končí. Zbývá jen opětovně připomenout, že v šestnáctém století žádný zákon o ochraně osobních údajů neexistoval. Všichni odpovědní činitelé té doby se tudíž pouze tvářili, jako by se na předchozích řádcích popisované události vůbec nestaly.

JM