DIGITÁLNÍ SBÍRKY A DATA

Elektronické databáze osobních údajů

Jan Folda
jan.folda@sos-vesnicky.cz

Žijeme ve světě, který je stále více závislý na počítačových technologiích. Nevyhnutelným důsledkem této skutečnosti jsou i stále výraznější snahy o vývoj nástrojů, s jejichž pomocí bude možné popsat nebo dokonce předvídat chování jednotlivce nebo společnosti jako celku pomocí přesně definovaných matematických vztahů. Součástí tohoto trendu je i obrovský rozmach informačních databází obsahujících osobní údaje, které představují kvalitativně zcela novou úroveň ve srovnání s dobou ještě nedávno minulou. Základní změnou je především převod databází do elektronické podoby. Ruku v ruce s touto proměnou se však vynořuje dosud nebývalá hrozba pro soukromí každého z nás. Existence informačních databází v elektronické podobě totiž neznamená pouze možnost rychlého a snadného vyhledání požadovaných údajů. Stejně tak se objevuje i riziko odcizení databáze obsahující osobní údaje s cílem tyto údaje zneužít pro kriminální aktivity. Osobní údaje obsažené v různých databázích je také možné snadno kombinovat či srovnávat. Výsledkem může být mimořádně závažný průnik do soukromí. Je proto třeba nastavit přesná pravidla fungování takovýchto databází, aby rizika vyplývající z jejich existence a provozu byla pokud ne zcela eliminována, tak alespoň omezena na minimum.

Práva a povinnosti při vytváření databází osobních údajů

V podmínkách České republiky je základním právním ustanovením, které stanovuje pravidla pro vytváření databází osobních údajů, zákon č. 101/2000 Sb., o ochraně osobních údajů. Tato norma primárně zakotvuje zásadu, že osobní údaje smí být shromažďovány a dále systematicky zpracovávány jen se souhlasem subjektu údajů, pouze v zákonem vymezených případech pak i bez tohoto souhlasu. Souhlas ze zpracováním osobních údajů by měl být vědomým, svobodným a informovaným projevem vůle jednotlivce. Situace jako z westernového příběhu, kdy hlavní bandita drží hrdinovi u hlavy zbraň a nutí ho podepsat prázdný papír, zákon nepřipouští. Nemusíme ale chodit až na daleký Divoký západ, abychom si představili situaci, která bude odporovat zákonu. Vždyť kolikrát se vám již stalo, že od vás byly požadovány vaše osobní údaje (nejčastěji rodné číslo), aniž byste byli informováni, za jakým účelem, na jak dlouho a kdo přesně od vás tyto údaje chce získat? Všechny tyto informace byste přitom měli dostat předtím, než své údaje poskytnete.

Mnoho z nás si jistě vzpomene na situaci, kdy své osobní údaje poskytli dobrovolně a jako „protihodnotu“ získali nějakou konkrétní výhodu či odměnu. Typickým příkladem takové situace jsou různé marketingové databáze obchodních řetězců (věrnostní karty), evidence vítězů soutěžních her nebo databáze držitelů In karty Českých drah. Součástí formuláře, jehož prostřednictvím své osobní údaje poskytujete, samozřejmě musí být poučení o tom, komu, na jak dlouho a za jakým účelem své osobní údaje poskytujete. A právě tady se objevuje jeden z nejčastějších problémů. Mnoho lidí totiž své osobní údaje poskytuje bez valné

kontroly, aniž by si pečlivě přečetli celý text souhlasu se zpracováním osobních údajů. Po určité době jsou překvapeni množstvím reklamních materiálů, které jim jsou zasílány poštou, nebo tím, že jim neznámé osoby volají na jejich soukromá telefonní čísla. Neuvědomí si, že v minulosti poskytli svůj souhlas se zasíláním reklamních materiálů nejen společnosti, která od nich souhlas získala, ale např. i jejím obchodním partnerům. Jednoduchá rada, která zde může zaznít, proto je – vždy si pečlivě zkontrolujte, k čemu přesně dáváte svůj souhlas! Souhlas se zpracováním osobních údajů je samozřejmě možné odvolat. Příslušná evropská směrnice výslovně stanoví, že by se mělo jednat o jednoduchý úkon, ale často se naopak jedná o uměle komplikovanou proceduru, která pro dotčeného jedince znamená nejen časovou, ale především velkou nervovou zátěž.

V předchozím textu bylo řečeno, že existují i situace, kdy zákon připouští shromažďování a další systematické zpracování osobních údajů bez souhlasu subjektu údajů. Typickým příkladem, kdy není vyžadován souhlas subjektu údajů, je zpracování osobních údajů v situaci, kdy je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Právě sem patří v poslední době tolik populární kamerové systémy vybavené záznamovým zařízením, sloužící k ochraně majetku. Poměrně běžně se objevuje mylný názor, že jestliže kamerový systém slouží k ochraně majetku, je možné ho nainstalovat a uvést do provozu bez nutnosti splnit nějaké další povinnosti. Tak tomu ale samozřejmě není. V okamžiku, kdy je kamerový systém vybaven záznamovým zařízením, jedná se o zpracování osobních údajů, a proto je třeba dodržet povinnosti vyplývající ze zákona o ochraně osobních údajů. Provozovat takový kamerový systém lze proto bez souhlasu subjektu údajů pouze v přesně stanovených situacích, kdy je skutečně jediným účelem ochrana majetku, zdraví, života apod. Rozhodně nelze připustit provozování kamerového systému se záznamem např. na pracovištích v době, kdy jsou přítomni zaměstnanci, nebo v prostorách převlékáren bazénů, fitness center apod. Sledování zaměstnanců na pracovišti (např. s pomocí kamerového systému) navíc v současnosti zakazuje i zákoník práce. Výjimku představují pouze situace, kdy **u zaměstnavatele existuje závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele (např. banky, směnárny apod.)**. Argument zaměstnavatele, že pomocí kamerového systému chce kontrolovat, zda jeho zaměstnanci skutečně pracují, jakoby vypadl z románu „1984“ G. Orwella. Jiná situace samozřejmě nastává, pokud skutečně není v silách zaměstnavatele zajistit zabezpečení svého majetku jinou cestou. Typickým příkladem jsou kamerové systémy v obchodech nebo bankách. Zaměstnanci i zákazníci ale musí být v takovém případě na přítomnost kamerového systému viditelně upozorněni. V případě převlékáren např. v plaveckém bazénu je situace obdobná. Instalace kamer je sice možná, ale vždy musí být zajištěn prostor, kam kamery nevidí, a zároveň musí být návštěvníci na přítomnost kamerového systému upozorněni.

V běžném životě se ale můžeme setkat i s mnoha dalšími případy, kdy není vyžadován náš souhlas se zpracováním osobních údajů. Zmiňme např. nástup do nového zaměstnání, kdy zaměstnavatel vyžaduje sdělení poměrně velkého počtu osobních údajů, aniž by si současně vyžádal náš souhlas s jejich zpracováním. Zpracování osobních údajů je v tomto případě nezbytné pro jednání o uzavření nebo změně smlouvy, a proto udělení souhlasu není třeba. Zaměstnavatel je však samozřejmě oprávněn zpracovávat jen osobní údaje nezbytně nutné ke stanovenému účelu. Dalším příkladem může být jednání o zřízení bankovního účtu nebo poskytnutí úvěru, kdy od nás banka také požaduje sdělení velkého množství osobních údajů. Banky mají ze zákona povinnost pro účely bankovních obchodů zjišťovat a zpracovávat údaje o osobách včetně rodného čísla, pokud bylo přiděleno, vyjma citlivých údajů o fyzických

osobách. Ani v tomto případě tedy není souhlas subjektu údajů se zpracováním osobních údajů vyžadován. Nelze opomenout, že do této kategorie, tedy zpracování osobních údajů za účelem dodržení právní povinnosti správce, patří i valná část databází osobních údajů, kterými disponuje stát a orgány veřejné správy (evidence obyvatel, příjemci dávek sociální podpory, rejstřík trestů, evidence držitelů živnostenského oprávnění, katastr nemovitostí atd.).

Bez souhlasu subjektu údajů lze také zpracovávat osobní údaje, pokud se tak děje výlučně pro účely archivnictví podle zvláštního zákona. I zde platí podmínka, že by tvůrce takovéto databáze měl dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.

Je třeba zdůraznit, že ani v situacích, kdy není vyžadován souhlas se zpracováním osobních údajů, nemizí informační povinnost správce. Subjekt údajů má tedy právo být informován o tom, komu své osobní údaje poskytuje, resp. po jakou dobu a za jakým účelem budou zpracovávány.

Správci osobních údajů jsou ze zákona vázáni řadou různých povinností. Mezi zcela zásadní patří především povinnost vést pouze přesné osobní údaje, které byly získány v souladu se zákonem. Typickým příkladem situace, kdy se správce dostal do rozporu s touto povinností, je databáze plátců koncesionářských poplatků České televize a Českého rozhlasu. Svým rozsahem patří tyto databáze mezi největší databáze osobních údajů v České republice, a proto je již na základě statistické pravděpodobnosti možné určitou míru chybovosti předpokládat. Při velké kampani zaměřené na neplatiče koncesionářských poplatků, která v nedávné minulosti proběhla, se potvrdilo, že údaje v databázi obsažené byly sice získány v souladu se zákonem, ale zároveň bylo zjištěno, že množství chybných záznamů v databázích přesahuje statisticky předvídanou míru chybovosti. Česká televize i Český rozhlas proto byli nuceni z pozice správce vyvinout aktivní snahu vedoucí k nápravě tohoto stavu.

Jestliže je zjištěno, že osobní údaje jsou přesné a byly získány v souladu se zákonem, neznamená to, že správce databáze splnil všechny své povinnosti. Nelze zapomenout na povinnost shromažďovat a následně zpracovávat osobní údaje pouze v souladu se stanoveným účelem a v rozsahu nezbytném pro naplnění stanoveného účelu. Výjimku z tohoto pravidla představují pouze specifické situace uvedené v zákoně, z nichž dnes asi nejznámějším příkladem jsou činnosti spojené se zpřístupňováním svazků bývalé Státní bezpečnosti. V jiných případech musí správce získat se zpracováním osobních údajů k jinému účelu než byl původně stanovený souhlas subjektu údajů. Údaje, které byly získány k rozdílným účelům, také nesmí být sdružovány. Jestliže tedy správce vede dvě nebo i více různých databází osobních údajů, které byly zřízeny za různým účelem, je nepřípustné údaje v těchto databázích propojovat a vytvářet tak databázi novou. Zároveň se stanovením účelu zpracování osobních údajů musí správce také stanovit dobu, po kterou budou osobní údaje zpracovávány. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, vědecké účely a pro účely archivnictví. Jako poslední, ale rozhodně neméně významnou povinnost pak připomeňme povinnost správce osobních údajů provést všechna nezbytná opatření k zabezpečení vznikající databáze osobních údajů. Rozumí se tím např. nastavení režimu přístupu k údajům, mechanické zabezpečení, v případě elektronických databází dostatečně silné šifrování apod. V posledních měsících téměř nemine týden, aby svět neobletěla zpráva o úniku velkého množství osobních údajů z nějaké informační databáze. Nejčastěji se jedná o výsledek kriminálních aktivit (především v případě databází bankovních institucí) nebo

prosté lidské chyby. Nezapomeňme, že dnes již mnoho lidí má svou identitu, resp. její přesný „otisk“ v prostředí různých elektronických databází, někteří lidé mají dokonce identit několik (skutečnou a pak jednu nebo dokonce několik virtuálních). Ve vyspělých zemích je pak v souvislosti s nedokonalým zabezpečením databází osobních údajů stále častěji skloňován nový pojem – krádež identity. Situace, kdy někdo okopíruje „vaši“ identitu a vydává se za vás, je jen těžko představitelná, přesto k tomu již dochází. Smutnou pravdou je, že cena takto odcizené kompletní identity je velmi nízká (maximálně stovky amerických dolarů) a počet případů krádeže identity roste raketovým tempem. Vedle vážných osobních problémů pak taková situace často znamená i velké finanční ztráty (ze zahraničních údajů vyplývá, že se často jedná o částky ve výši desítek tisíc amerických dolarů). Neustále je třeba si připomínat, že osobní údaje představují skutečný klíč k našemu soukromí a v mnoha případech slouží ke vstupu do různých databází. Jakmile tyto údaje neopatrně předáme do nesprávných rukou, následky mohou být dalekosáhlé a náprava prakticky nemožná.

Zneužití databází osobních údajů v minulosti

Dosud jsme v textu hovořili pouze o tom, jaká pravidla by měla být respektována, aby nedošlo k chybnému nakládání s databázemi osobních údajů nebo přímo k jejich zneužití. Tato pravidla vycházejí mimo jiné z historické zkušenosti, kterou získala Evropa v dobách druhé světové války. Nacistické Německo rozpoutalo do té doby těžko představitelné pronásledování vlastního obyvatelstva židovského vyznání, které posléze rozšířilo i na všechna území v Evropě obsazovaná během válečných tažení. Jako významná pomůcka přitom posloužily existující databáze osobních údajů, ať již se jednalo o výsledky sčítání lidu nebo zvláštní seznamy členů židovské obce. Paradoxně přitom nedošlo k porušení platného práva, neboť nacistický režim deformoval právní stav v Německu natolik, že pronásledování a posléze i přímá fyzická likvidace Židů a dalších „méněcenných“ obyvatel nebyla v rozporu s žádným z platných zákonů, kromě obecně platných zákonů morálky a slušnosti. Na ty se ale nacistický režim pramálo ohlížel. Na základě platné legislativy nejen že nesměli Židé vykonávat řadu povolání a byla jim upřena i účast na vzdělávání či kulturních akcích, ale jejich identifikační průkazy byly doplněny o velké písmeno „J“ značící osobu židovského vyznání. Stejným způsobem byly upraveny i cestovní doklady. Od roku 1938 byly Židům vydávány zvláštní identifikační doklady a zároveň museli Židé přijmout ke svému dosavadnímu jménu nové „židovské prostřední jméno“ (Sarah pro ženy a Israel pro muže) (obr. 1).

Efektivita ve využívání shromážděných informací o obyvatelstvu byla v nacistickém Německu a později i na německou armádou obsazených územích děsivá. Mezi nejčastěji uváděné příklady patří události v Nizozemsku, kde byly podle výsledků sčítání lidu vytvořeny seznamy veškerého židovského obyvatelstva a na základě těchto seznamů byly od července roku 1942 zahájeny deportace židovského obyvatelstva do koncentračních táborů. Z celkového počtu 140 000 registrovaných obyvatel židovského vyznání se po válce do svých domovů nevrátilo 102 000 osob, tedy 73 %! Mezi nejznámější oběti patří rodina Anny Frankové, která se dlouhou dobu skrývala a v tomto úkrytu vznikl i slavný Deník malé Anny.

Historická zkušenost holocaustu, kdy i kvůli děsivě účinnému systému zneužívání existujících databází osobních údajů zahynulo možná až 6 000 000 osob židovského vyznání, jasně upozornila na skutečnost, že s využitím moderních prostředků lze snadno a rychle shromáždit velké množství osobních údajů. Není proto překvapením, že se součástí Všeobecné deklarace lidských práv vydané 10. prosince 1948 Organizací spojených národů stal i článek 12, který říká:

„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst.

Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“

Bohužel ani iniciativy OSN a dalších mezinárodních organizací nezabránily dalším a dalším pokusům o zneužití osobních údajů či o neoprávněné zasahování do soukromí. S rozvojem moderních prostředků komunikace a vznikem elektronických databází osobních údajů je naopak toto riziko ještě větší než kdykoliv v minulosti.

Elektronické databáze osobních údajů

Současný svět asi nejlépe charakterizuje slovo rychlost. Každý někam spěchá, neustále se objevují nové a nové časové termíny, do kdy musí být něco hotovo, zprávy z jednoho konce světa na druhý putují doslova rychlostí blesku. Stejně tak rychle ale mohou putovat do nepovolaných rukou osobní údaje, zvláště pokud jsou uloženy v elektronických databázích. V následujících odstavcích se zaměříme na nejvýznamnější rizika a na konkrétních příkladech se pokusíme předvést, jaká je současná praxe při tvorbě a provozování elektronických databází osobních údajů.

Jestliže hovoříme o elektronických databázích, většina lidí si asi představí databáze s propojením na počítačovou síť internet. Zdaleka ne vždy to platí, i bez připojení databáze k internetu se však objevuje řada rizik, která nelze podceňovat. Velmi často se např. můžeme setkat s tím, že správce elektronické databáze osobních údajů není schopen prokázat udělení souhlasu subjektu údajů se zpracováním jeho osobních údajů. Vzhledem k charakteru databáze totiž často dochází k udělení souhlasu elektronickou cestou (e-mail, odpovědní formulář apod.) a jeho prokazatelnost tak může být sporná. Správce databáze osobních údajů by však měl být v každém okamžiku schopen prokázat, že souhlas skutečně poskytl příslušný subjekt údajů. Jistotu, že souhlas skutečně poskytla osoba X, správce databáze získá jen v případě e-mailové zprávy podepsané zaručeným elektronickým podpisem. V ostatních případech musí alespoň platit pravidlo, že přednastavená volba v elektronických formulářích o udělení souhlasu se zpracováním osobních údajů zní „nesouhlasím“. Subjekt údajů tak musí sám zaškrtnout volbu „souhlasím“ a správce osobních údajů následně ještě na zadané kontaktní údaje zašle potvrzující e-mail s dotazem, zda souhlas skutečně poskytl dotčený subjekt údajů. V případě, že by toto pravidlo nebylo dodržováno, hrozilo by riziko, že bude možné předat osobní údaje cizí osoby do mnoha různých databází, aniž by se tato o tom vůbec dozvěděla. Riziko samozřejmě není ani při použití výše popsaného modelu zcela eliminováno, neboť stále existuje možnost, že do elektronického formuláře bude zadána např. falešná e-mailová adresa, ze které pak bude odesláno i požadované potvrzení se souhlasem se zpracováním osobních údajů. Zcela jednoznačné potvrzení by bylo možné získat jen v případě, kdy by správce osobních údajů po získání elektronického souhlasu požádal v potvrzujícím e-mailu subjekt údajů o zaslání souhlasu v písemné podobě.

Vedle rizika, že souhlas se zpracováním osobních údajů poskytne někdo jiný než skutečný nositel údajů, nesou elektronické databáze i další hrozby. Zcela specifickým rizikem, vlastním pouze databázím vedeným v elektronické podobě, je riziko odcizení, resp. zneužití údajů z databáze prostřednictvím dálkového přístupu přes počítačovou síť internet. S touto hrozbou samozřejmě souvisí i otázka zabezpečení databáze. V případě elektronických databází se jedná především o dostatečně silné šifrování a nastavení režimu přístupu k údajům,

ale opomenout nelze ani zabezpečení mechanické. V České republice jsme již zaznamenali případy, kdy se správce osobních údajů domníval, že databázi osobních údajů odpovídajícím způsobem zabezpečil díky využití silného šifrování. Zcela nedostatečné však bylo mechanické zabezpečení (uzamčení přístupu k přístupovému terminálu) a neznámý zloděj si tak celou „dokonale" zabezpečenou databázi bez větších problémů odnesl na několika záznamových médiích. I soud nakonec ve svém rozsudku potvrdil, že správce osobních údajů v tomto případě neprovedl všechna nezbytná opatření k ochraně shromážděných osobních údajů. Mediálně známější jsou však případy, kdy – ať již vlivem lidské chyby nebo s využitím kriminálních praktik – unikne do počítačové sítě Internet často obrovské množství osobních údajů. Velmi oblíbeným cílem kriminálních živlů jsou především finanční instituce, neboť získat přístup k bankovním záznamům samozřejmě znamená reálnou možnost významného finančního zisku. Téměř stejně často ale můžeme číst i o tom, že unikly osobní údaje ze systémů poskytovatelů e-mailových služeb nebo různých personálních agentur. Obrovské nebezpečí těchto bezpečnostních trhlin spočívá v tom, že údaje jednou uniklé do počítačové sítě Internet se prakticky nedají „lapit" zpět. V mnoha případech pak mohou jejich nositelé opakovaně zažívat nepříjemné situace, kdy jsou spojováni s událostmi, se kterými ve skutečnosti nic společného nemají, nebo jsou na jejich jméno objednávány různé služby apod. Řada lidí se také velmi obtížně vyrovnává s tím, že mnohdy unikají i velmi intimní informace (především v případě krádeže či úniku dat ze systémů e-mailové pošty).

Na druhou stranu nelze pominout skutečnost, že řada lidí úniku svých osobních údajů aktivně napomáhá. Stále více z nás se smiřuje s tím, že existuje velké množství různých elektronických databází, které obsahují naše osobní údaje a do kterých máme sami přístup prostřednictvím internetu. Netrvalo dlouho a objevila se podoba počítačové kriminality, která se tohoto faktu pokouší využít. V nedávné době proběhla i českými médii série zpráv o tom, jak velké množství lidí obdrželo do své e-mailové pošty zprávu, která vypadala jako oficiální výzva jejich banky, aby potvrdili své přístupové údaje do systému elektronického bankovnictví. Přestože banky (ani jiní poskytovatelé elektronických systémů obsahujících osobní údaje) nikdy podobné výzvy elektronickou cestou nezasílají a opakovaně na to upozorňují, někteří lidé na tuto výzvu zareagovali. Až posléze zjistili, že se ve skutečnosti jednalo o formu zločinu, která se označuje jako phishing, česky rybaření. Cílem je nabídnout nic netušící oběti podvodnou internetovou stránku, která se tváří jako pravá stránka např. systému elektronického bankovnictví, a jejím prostřednictvím vylákat přihlašovací údaje k bankovnímu účtu. Ten je následně vykraden a poškozenému zůstávají jen oči pro pláč. Jindy se můžeme pro změnu setkat se situací, kdy lidé využívají nabídky internetových obchodů nebo jiných online služeb, přestože jejich stránky nejsou dostatečně zabezpečeny proti „odposlechu" informací zasílaných prostřednictvím internetu. Jestliže se potom tito lidé na takové stránce registrují, všechny osobní údaje, které v průběhu registrace zadávají, mohou být zachyceny někým nepovolaným a následně zneužity. Proto je třeba neustále opakovat, že nejen správci databází osobních údajů mají své povinnosti. Každý, kdo se rozhodne využívat elektronické systémy obsahující osobní údaje, by měl dbát elementárních pravidel bezpečnosti.

Dalším příkladem, kdy uživatelé svou vlastní neopatrností umožní únik svých osobních údajů, je neopatrnost při prodeji použité výpočetní techniky. Původní majitel přitom jednoduše smaže data uložená na pevném disku počítače a domnívá se, že tím učinil nezbytným bezpečnostním opatřením zadost. Ve skutečnosti jsou ale tato data snadno obnovitelná. Dokonce dnes existují specializované kriminální skupiny využívající data získaná z použité výpočetní techniky ke krádežím finančních prostředků z bankovních účtů nebo k vydírání.

V následujícím textu se blíže zaměříme na některé konkrétní příklady elektronicky vedených databází osobních údajů. Některé z nich můžeme považovat za příklady toho, jak by měly elektronicky vedené databáze osobních údajů vypadat, jiné jsou naopak negativním příkladem, tedy jak by elektronické databáze osobních údajů rozhodně vypadat neměly.

Databáze DNA

Molekula DNA, která je nositelem genetické informace všech organismů s výjimkou těch nebuněčných organismů, u nichž hraje tuto úlohu RNA, byla objevena již v roce 1869, její charakteristickou strukturu se ale podařilo objevit až v polovině 20. století. V roce 1985 pak byla na univerzitě v Leicestru ve Velké Británii objevena metoda genetické daktyloskopie, která využívá analýzu DNA k jednoznačné identifikaci osob. Již rok po svém objevu byla tato metoda využita v rámci kriminalistického vyšetřování. Dnes se vedle kriminalistiky využívá analýza DNA také při zjišťování otcovství, v lékařském výzkumu nebo při genografických testech (pomocí těchto testů lze zjistit, ze které části světa pocházeli předci testované osoby). Metod, které se k analýze DNA používají, bylo vyvinuto mnoho, nicméně v současnosti se prakticky standardní metodou stalo určování tzv. STR polymorfismů. Při této metodě se vychází z faktu, že šroubovice DNA obsahuje místa, která nekódují nějaký konkrétní genetický znak, ale tvoří je náhodně se opakující série jakéhosi „slova“, které tvoří mnohokrát opakovaný sled 2–4 nukleotidů. Tyto sekvence označujeme jako tandemové repetice a v lidské DNA jich známe více než 8 tisíc. Podoba těchto repetic a jejich délka je výrazně individuální a právě toho využívá i metoda STR polymorfismů. Pro účely sestavení DNA profilu je tak vybráno několik konkrétních tandemových repetic, jejichž počet se liší podle použité metodiky. Např. systém CODIS, využívaný americkou FBI, pracuje s 13 úseky DNA, navíc se ještě zjišťuje genetický znak, který kóduje pohlaví. Česká policie pracuje s 15 úseky (a s genetickým znakem pro určení pohlaví), naproti tomu systém SGM+ ve Velké Británii využívá pouze 10 úseků (a opět plus genetický znak pro určení pohlaví). Výsledný genetický profil nám s výjimkou informace o pohlaví zjišťované osoby neříká nic o jejích genetických predispozicích, umožňuje ale její jednoznačnou identifikaci. Pravděpodobnost, že dvě osoby budou mít stejný genetický profil, je udávána poměrem více než 1:500 miliardám a jedinou známou situací, kdy k tomu dochází, jsou jednovaječná dvojčata.

Vzhledem k úspěchům, kterých policie díky analýze DNA začala dosahovat při odhalování dosud neobjasněných případů, nebylo překvapením, že se objevily snahy vytvořit databázi profilů DNA, která by posloužila jako srovnávací základna při každém dalším vyšetřování. První taková databáze byla zprovozněna ve Velké Británii (Národní databáze DNA) v roce 1995 a dnes je tato databáze největší na světě, když zahrnuje více než 5 % populace Velké Británie. Podobné databáze vznikají i v mnoha dalších zemích světa včetně České republiky (tzv. Národní databáze DNA dnes zahrnuje cca 0,2 % populace ČR). V souvislosti se vznikem těchto databází se ale vynořily do té doby neznámé problémy. Pravděpodobně nejzávažnější skutečností je fakt, že k zařazení do kriminalistické databáze DNA často stačí pouhá přítomnost na místě činu (nemusíte tedy být ani pachatelem nebo obětí, stačí, že jste byli svědky trestného činu). Navíc se v některých zemích (nejsilněji ve Velké Británii) objevují snahy zařadit do kriminalistické databáze DNA veškerou populaci daného státu. Přestože zatím tyto snahy neopustily stadium úvah, rozhodně stojí za pozornost. Postupně totiž vzniká společnost apriori podezřelých, neboť, pokud by podobné úvahy byly jednou skutečně realizovány, každý z nás by byl při spáchání každého závažnějšího trestného činu prověřován jako potenciální pachatel. Vedle kontroverzních otázek souvisejících s rozsahem databáze se často hovoří také o nevyváženém podílu některých věkových a etnických skupin

v kriminalistických databázích DNA. Výzkumy z Velké Británie tak např. varují před vysokým podílem mladých černošských mužů v databázi, který neodpovídá jejich podílu na celkové populaci.

Vedle databází sloužících potřebám kriminalistického vyšetřování vznikají i další databáze DNA. Nejčastěji se jedná o databáze pro potřeby lékařského výzkumu nebo genografické databáze. Lékařský výzkum se v posledních letech zaměřuje na vývoj léků, které budou přizpůsobené konkrétním jednotlivcům nebo skupinám osob. K tomu je samozřejmě třeba získat dostatečně rozsáhlou srovnávací základnu genetických výbav těchto jedinců. Nejrozsáhlejší databáze tohoto druhu vzniká na Islandu. Podle původních plánů měla zahrnout veškerou populaci. Nakonec se ale od těchto plánů ustoupilo a předání vzorku do databáze je dobrovolné. Další podobně ambiciózní projekt vzniká ve Velké Británii, v menším měřítku takové databáze najdeme i v jiných zemích světa.

Pod pojmem genografické databáze rozumíme databáze profilů DNA, kdy na základě zjištění tzv. Y-haplotypu (část DNA, která se dědí jen v mužské linii a je proto téměř neměnná) dochází ke zjišťování oblasti původu předků (cca 50–60 generací zpět). Na rozdíl od lékařských databází se nejedná o detailní rozbor DNA. Právě na příkladu genografických databází si ale můžeme ukázat nejvážnější rizika spojená s databázemi DNA. Zatímco původní vzorky DNA jsou (nebo přesněji měly by být) po provedení analýzy zničeny, výsledek je v elektronické podobě zařazen do databáze. Databáze DNA jsou ze své podstaty konstruovány tak, aby bylo možné v nich snadno vyhledávat a porovnávat uložené profily DNA. Naplňují tak přesně definici elektronické databáze osobních údajů a jako zcela zásadní se proto při vytváření databází DNA jeví jasné právní vymezení jejich fungování. Zatímco v zahraničí již takovéto zvláštní právní normy v mnoha případech existují, v České republice tomu tak zatím není a klíčovou právní normou tak zůstává zákon o ochraně osobních údajů č. 101/2000 Sb. I proto se objevuje řada pochybností o fungování některých databází DNA. Velmi problematické se často ukazují např. testy paternity (otcovství), neboť zatímco renomované laboratoře pracují pouze se vzorky, u nichž současně obdrží souhlas subjektu údajů (v tomto případě tedy potenciálního otce, resp. i matky), existují i na českém trhu firmy, které jsou ochotné zpracovat testy, aniž by se otázkou souhlasu subjektu údajů vůbec zaobíraly. Vzorky navíc často zasílají ke zpracování do zahraničí a nikde nenajdeme jistotu, že výsledky dané analýzy nejsou ukládány do nějaké databáze, kde slouží např. k lékařskému výzkumu. Všechny tyto aspekty by si měl člověk, který je rozhodnut testování DNA podstoupit dobrovolně (v případě kriminalistických databází je tomu samozřejmě jinak), velmi dobře rozmyslet a především by si měl velmi pozorně přečíst, k čemu uděluje svůj souhlas! Nezapomeňme, že v posledních dnech se na českém trhu objevila i společnost, která nabízí testování „podezřelých“ skvrn na oblečení či povlečení za účelem zjištění cizí DNA. Výsledkem pak má být odhalení případné nevěry. Spoléhat proto na dodržování platného práva a slušnost bez příslušné kontroly se v oblasti testování DNA určitě nedoporučuje.

Kromě problémů vyplývajících z chybějícího právního rámce pro databáze DNA se však objevují i další rizika. Asi nejvážnějším je případné chybné nastavení bezpečnostních oprávnění pro přístup nejen k výsledkům analýz, ale především k původním vzorkům. Pokud by se objevila možnost, že by se k vzorkům mohl dostat někdo nepovolaný, hrozilo by vážné riziko zneužití DNA. Nezapomeňme, že přítomnost DNA na místě činu je považována za téměř nevyvratitelný důkaz v soudním řízení. Pokud by tak někdo mohl bez potřebného oprávnění získat váš vzorek DNA původně odevzdaný např. kvůli testu otcovství, mohl by se z vás

během krátké doby stát nejen nečekaně otec (...), ale také člověk obviněný ze závažného trestného činu. Prokazovat, že jste daný trestný čin nespáchal, by pak mohl být velmi obtížný úkol. I proto je třeba velmi důsledně kontrolovat bezpečnostní parametry nakládání se vzorky DNA.

Jmenná evidence cestujících (PNR)

Další elektronickou databází osobních údajů, na kterou se zaměříme, je tzv. jmenná evidence cestujících (PNR = Passanger Name Records). Jedná se o databázi, která je výsledkem boje Spojených států proti terorismu po útocích z 11. září 2001, ale zároveň se jedná o jednu z nejkontroverznějších databází osobních údajů vůbec. Cílem je na základě analýzy údajů o cestujících a jejich plánované cestě určit míru rizika, kterou tito cestující představují, s cílem předcházet dalším možným teroristickým útokům.

První pokusy o hodnocení cestujících z hlediska možných rizik začaly ve Spojených státech již na konci 90. let v reakci na nárůst hrozby mezinárodního terorismu. Po událostech z roku 1996, kdy v průběhu několika po sobě následujících dnů došlo ke zřícení letadla společnosti TWA 800 (podezření na teroristický útok se nakonec nepotvrdilo) a bombovému útoku během olympiády v Atlantě, došlo v roce 1997 ke spuštění systému, který se označuje jako Počítačový systém předběžného hodnocení cestujících (CAPPS – Computer Assisted Passenger Prescreening System). Systém provozuje FBI a FAA (Federální úřad pro letectví) a je založen na analýze údajů o cestě, které běžně shromažďují letecké společnosti. Pokud je systémem některý z cestujících označen za potenciální hrozbu, musí i se svými zavazadly projít podrobnější kontrolou. Dne 11. září 2001 systém správně identifikoval jako hrozbu většinu atentátníků, ale protože jejich zavazadla prošla kontrolou bez problémů, byli všichni vpuštěni na palubu.

Poté, co se ukázalo, že systém CAPPS I nedokázal efektivně zabránit teroristickým útokům z 11. září, byla navržena nová generace systému pod názvem CAPPS II. Na rozdíl od původního systému měla být tato druhá generace provozována Ministerstvem pro vnitřní bezpečnost. Údaje o cestujícím získané při koupi letenky měly být porovnány s údaji uloženými v existujících vládních a komerčních databázích. Byla by tak ověřena totožnost cestujícího, jeho případné předchozí kriminální aktivity, ale také to, zda daný cestující nemá možné vazby na teroristy. Cestující by byl pomocí barevné škály ohodnocen z hlediska možné rizikovosti a toto hodnocení by bylo zasláno zpět letecké společnosti (obr. 2). Pokud by cestující v tomto hodnocení získal červený stupeň, pak po příchodu na letiště by byl ihned zatčen. V případě, že by cestující byl z hlediska rizika ohodnocen na oranžový stupeň, byl by nucen podrobit se zpřísněné kontrole. Standardně by byl cestující odbaven v okamžiku, kdy by získal hodnocení na úrovni zeleného stupně. Systém CAPPS II vzbudil velmi hlasité protesty ze strany ochránců lidských práv a nakonec byl plán na jeho vytvoření prezidentem Bushem v srpnu roku 2004 odvolán. Prakticky vzápětí, na počátku roku 2005, byl ale zrušený plán na vytvoření systému CAPPS II nahrazen novým programem pod názvem „Bezpečný let“. Tento program má za úkol prakticky totéž co zrušený program CAPPS II, ale vzhledem k pokračujícím protestům a obavám z narušování soukromí nebude ani tento program plně funkční dříve než v roce 2010. Před jeho uvedením do provozu bude také třeba odstranit problémy s často se opakujícím chybným označením nevinných cestujících za podezřelé. Asi nejznámějším případem bylo označení senátora Teda Kennedyho v roce 2004.

Z hlediska evropských cestujících se ukázal být jako přelomový rok 2003, kdy americká administrativa začala od evropských leteckých společností vyžadovat předávání údajů o cestujících. Letecké společnosti měly předávat americkým úřadům až 34 různých osobních údajů svých cestujících. Údaje musely být předány s dostatečným předstihem, aby mohli být cestující prověřeni. V případě neposkytnutí součinnosti si americké úřady vyhradily právo letecké společnosti pokutovat až do výše 5000 € za každého cestujícího na palubě letadla, resp. odmítnout povolení k přistání.

Evropské letecké společnosti se poté, co americké úřady vznesly požadavek na předávání osobních údajů cestujících leteckých společností, dostaly právně do velmi složité situace. Pokud by tomuto požadavku vyhověly a údaje předávaly, dostaly by se do rozporu s platnou evropskou legislativou o ochraně osobních údajů. Ochránci osobních údajů kritizovali především příliš široký rozsah požadovaných údajů, nedostatečně vymezený okruh orgánů, kterým se údaje zpřístupňují, a metodu „pull“, kdy americká strana sama vstupuje do databází leteckých společností a získává z nich požadované údaje. Pokud by předávání odmítly, hrozily by jim výše zmíněné sankce ze strany amerických úřadů. V roce 2004 proto byla nakonec uzavřena dohoda mezi EU a USA o předávání osobních údajů cestujících leteckých společností. Protože ale ne všechny letecké společnosti sbíraly ve svých rezervačních systémech požadované údaje, v drtivé většině případů odcházelo do Spojených států údajů méně.

Podpis dohody mezi Spojenými státy a Evropskou unií vzbudil rozsáhlé protesty v řadách ochránců soukromí a zanedlouho se do celé záležitosti vložil i Evropský parlament, který se obrátil na Evropský soudní dvůr s žalobami, v nichž se domáhal zrušení dohody. V květnu 2006 Evropský soud dohodu zrušil, ale ve snaze vyhnout se stavu právní nejistoty stanovil dobu 4 měsíců, během níž muselo být předávání osobních údajů do USA vyřešeno jiným způsobem. Na tomto rozsudku Evropského soudu bylo z pohledu ochrany osobních údajů nešťastné především to, že soud nerozhodoval o samotné podstatě problému, tedy zda lze tímto způsobem předávat osobní údaje evropských občanů do zahraničí, ale své rozhodnutí postavil na formálním právním argumentu, že Evropská komise dohodu opřela o neadekvátní článek smlouvy o Evropských společenstvích, a proto ji zrušil.

Na přelomu září a října 2006 byla uzavřena nová, tentokrát ovšem výslovně dočasná dohoda, která měla oběma stranám poskytnout dostatek času na definitivní právní řešení celé situace. V červnu 2007 pak byla uzavřena nová dohoda o předávání údajů z jmenné evidence cestujících leteckých společností ze zemí Evropské unie do Spojených států. I tato nová dohoda je však předmětem kritiky. Evropský parlament, jednotlivé národní úřady pro ochranu osobních údajů i různé občanské iniciativy ve svých kritických reakcích poukazují především na skutečnost, že doba, po níž budou údaje americkými úřady uchovávány, se prodlužuje na 7 let (původně 3,5 roku), a dalších 8 let budou uchovávány v „neaktivním“ stavu, kdy k nim bude možné získat přístup pouze na základě jasně zdůvodněné žádosti. K údajům navíc může přistupovat velmi široký a především nejasný okruh orgánů, neboť americké Ministerstvo pro vnitřní bezpečnost bude údaje moci poskytovat „na základě svého uvážení“ dalším vládním orgánům. Dalším silně kritizovaným bodem dohody je to, že místo relativně přesně vyjmenovaných 34 jednotlivých požadovaných údajů se v nové dohodě objevuje 19 „druhů informací“. Dochází tak ke slučování mnoha původních údajů do jednoho typu a nabízí se možnost zahrnout mezi požadované údaje i informace, které dosud vyžadovány nebyly.

Jmenná evidence cestujících, resp. databáze, kterou na základě údajů z ní získaných vytvářejí americké úřady (konkrétně Ministerstvo pro vnitřní bezpečnost), patří v současné době mezi největší databáze osobních údajů na světě. Z pohledu evropských standardů ochrany osobních údajů se bohužel jedná o databázi, která nesplňuje některé základní požadavky na ochranu soukromí jednotlivce. Předávání osobních údajů do Spojených států a s tím spojené zasahování do soukromí je ospravedlňováno bojem za demokracii a svobodu. Pokud bychom tento vývoj nechali bez povšimnutí, mohli bychom se jednou probudit v zemi, kde nikdo žádné soukromí nemá. Otázkou je, zda bychom pak ještě měli onu demokracii a svobodu ...

Schengenský informační systém

Předcházející příklady elektronických databází osobních údajů byly v mnohém varující. Ukázaly nám, že zdaleka ne vždy je prvotním zájmem správců takových databází chránit soukromí jednotlivce, naopak až nepříjemně často se soukromí ocitá v nebezpečném ohrožení. Naštěstí existují i databáze, které, přestože svým rozsahem patří k největším na světě, přistupují k otázce ochrany soukromí velmi dobře. Asi nejlepším příkladem pak může být Schengenský informační systém (SIS).

Jedná se o společný informační systém států schengenského prostoru, který prostřednictvím automatického vyhledávání zajišťuje přístup příslušných orgánů těchto států k záznamům o osobách a věcech při provádění hraničních kontrol, popř. jiných policejních a celních kontrol ve vnitrozemí, a řízení o udělování víz, vydávání povolení k pobytu a posouzení příslušnosti státu k vyřízení žádosti o azyl. Od 1. září 2007 se k Schengenskému informačnímu systému (SIS) připojily i státy vstupující do schengenského prostoru na konci roku 2007 (včetně České republiky), a počet států využívajících SIS tak stoupl na 24. Vzhledem k počtu států, které jsou k systému připojeny, a k množství úkolů, které má tento systém plnit, není překvapením, že Schengenský informační systém představuje v současné době jednu z největších existujících elektronických databází osobních údajů na světě.

Struktura SIS má hvězdicovitou podobu (obr. 3), kdy v každém členském státě existuje tzv. národní část (N.SIS) a výměnu informací mezi nimi zajišťuje tzv. technická podpůrná jednotka (C.SIS), která je umístěna ve Štrasburku. Kterýkoli schengenský stát může do SIS (prostřednictvím národní části tohoto systému) vložit záznam a ten je prostřednictvím centrální části systému převeden do jednotlivých národních databází, kde je – na základě konkrétní žádosti – zpřístupněn příslušným orgánům členských států. Protože Schengenský informační systém obsahuje obrovské množství osobních údajů, je vkládání i využívání záznamů v rámci těchto kategorií ze strany národních dozorových orgánů pro ochranu osobních údajů velmi důsledně kontrolováno. Riziko však nespočívá jen v neoprávněném využívání nebo zpřístupnění údajů uložených v SIS. Pokud by došlo např. ke krádeži nebo ztrátě osobních dokladů a ty by pak byly použity při páchání trestné činnosti, mohlo by dojít k situaci, že by do Schengenského informačního systému byl vložen záznam o původním držiteli těchto dokladů, aniž by ten ve skutečnosti něco spáchal. Při každém dalším pokusu o překročení hranic schengenského systému by se pak tento člověk jevil jako podezřelý. Plně v souladu s evropskými standardy ochrany osobních údajů je proto pro případ zpracování nadbytečných či nesprávných údajů anebo neoprávněného záznamu dotčené osobě (subjektu údajů) zaručena možnost dovolat se nápravy, a to buď přímou cestou u daného správce dat (obvykle policejní orgány) nebo prostřednictvím národních dozorových úřadů. Zároveň byl zřízen Společný kontrolní orgán (Joint Supervisory Authority, JSA), který sdružuje zástupce národních dozorových úřadů a je pověřen kontrolou centrální jednotky a řešením případných

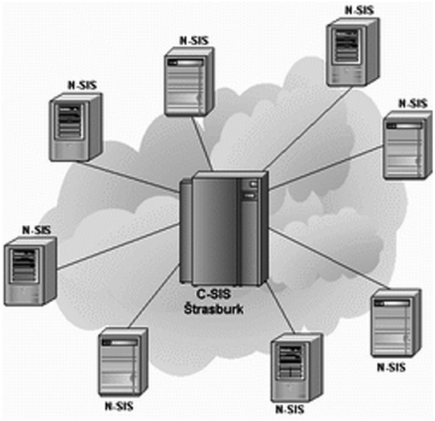
konfliktů mezi národními dozorovými úřady. Všechny dosavadní kontroly provedené jak na národní úrovni, tak i na úrovni celoevropské (technická podpůrná jednotka) prokázaly, že osobní údaje v Schengenském informačním systému jsou zpracovávány v souladu s platnou legislativou o ochraně osobních údajů.

Závěr

V předcházejících řádcích jsem se snažil představit základní principy, které by měly být dodržovány při shromažďování a následném zpracování osobních údajů prostřednictvím elektronických databází. Na konkrétních příkladech jsem se pak pokusil ukázat, že zdaleka ne vždy jsou požadované standardy ochrany osobních údajů důsledně dodržovány. Nepropadejme ale panice – téměř vždy máme možnost volby. Je ale nutné pozorně sledovat, k čemu dáváme svůj souhlas, resp. musíme si být vědomi svých práv. Jejich důsledné vymáhání je totiž jedinou cestou, jak si uchovat svoje soukromí alespoň částečně skutečně soukromé a nezměnit ho ve veřejné tajemství.

obr. 1
Identifikační průkaz, vydávaný od roku 1938 osobám židovského vyznání
zdroj: http://exlibris.memphis.edu/Secher-Schab/kennkart.htm (8. 10. 2007)

obr. 2
Návrh systému CAPPS II
zdroj: http://www.dontspyon.us/chart.html (9. 10. 2007)



obr. 3
Struktura Schengenského informačního systému
zdroj: http://www.integrace.cz/integrace/clanek.asp?id=316 (10. 10. 2007)