

úřad  
pro ochranu  
osobních  
údajů

# informační bulletin

## 2 / 2004

### Přivítací dopis novým členům EU

12. května 2004

Určeno: všem novým členům Pracovní skupiny Evropské komise zřízené podle článku 29

Vážení členové,

dne 1. května 2004 občané po celé Evropě nadšeně oslavili rozšíření Evropské unie při příležitosti přistoupení deseti nových členských států. Vaše země se nyní stala plnoprávným členem Evropské unie. Mnoho let přípravy a těžkostí tak dospělo k závěru a Vaše úsilí připojit se k rodině evropských národů jako rovnocenný partner přineslo plody.

Z titulu funkce předsedy a místopředsedy Pracovní skupiny podle článku 29 Vám blahopřejeme při příležitosti této vskutku historické události a sdílíme v této pohnuté chvíli Vaši radost. Nechť se všechny touhy Vaší země v budoucnosti uskuteční.

Je nám potěšením srdečně Vás přivítat jako nové členy této skupiny. Úkoly naší skupiny jsou mnohotvárné a náročné. Záležitostí, kterými se zabýváme, je stále více a zároveň jsou stále složitější. Jsme přesvědčeni, že nové členské státy dodají naší skupině impuls a obohatí naši práci novými myšlenkami a novými koncepcemi. Již jako pozorovatelé jste úspěšně přispívali k naší práci a nyní si můžeme vážit Vaší ještě aktivnější účasti v této skupině. Máme zájem na sdílení Vašich zkušeností týkajících se implementace Směrnice EU a stejně tak budeme naslouchat Vaším problémům a stížnostem.

Společným úsilím a v duchu evropské spolupráce ponese na svých bedrech budoucí úkoly a budeme hledat nejlepší možná řešení v zájmu našich občanů.

Velice se těšíme na další spolupráci s Vámi a přejeme Vám vše nejlepší do budoucna.

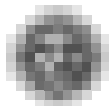
S přátelským pozdravem

Peter Schaar  
předseda

José Luis PIÑAR MAÑAS  
místopředseda

### TADY A TEĎ

Dne 1. června 2004 uplynuly 4 roky od vzniku Úřadu pro ochranu osobních údajů. Za tuto dobu česká instituce zřízená zákonem o ochraně osobních údajů a vykonávající dozor nad ochranou osobních údajů v České republice dokázala srovnat krok s partnerskými úřady v Evropě tradičních demokracií: Legislativním procesem prošla novela českého zákona o ochraně osobních údajů. Z hlediska evropské legislativy je jakousi poslední tečkou za supervizí zákona i fungování jím zřízené dozorné instituce. Svého druhu nakročením navíc je přiřazení genetických a biometrických údajů mezi obzvláště přísně chráněné citlivé údaje, což je změna, kterou novela uvedeného zákona č. 101/2000 Sb. rovněž přináší. Touto úpravou jsou už zohledňována i nebezpečí, která mohou ohrožovat soukromí i integritu osobnosti občana z hlediska nejspíše nejnovějších světových poznatků.



Pro svou práci Úřad využívá množství zahraničních kontaktů, které vybudoval za dobu své existence. Květnové setkání ochránců osobních údajů skupiny zemí V4, Pobaltí a Bulharska se uskutečnilo v Rize. Diskuse se dotýkala především řady společných nebo obdobných problémů, s nimiž se státy této skupiny v oblasti ochrany osobních údajů setkávají (jako konkrétní příklad lze uvést z hlediska ochrany osobních údajů problematické působení společnosti Vegas), ale také problémů, které aktuálně vyvstávají v ochraně osobních údajů i v jiných zemích – jako např. předávání osobních údajů leteckých pasažérů do USA a problematičnost služby Gmail nabízené společností Google.

Zároveň však je už Úřad v zahraničí vnímán jako instituce, která má ze svých znalostí co nabídnout: Na závěr projektu realizovaného v rámci programu Phare se španělskou Agenturou na ochranu dat, bylo podepsáno memorandum o další spolupráci mezi oběma institucemi, v němž deklarují zájem nadále spolupracovat na společném předávání zkušeností v oblasti ochrany osobních údajů ve státech východní Evropy a Balkánu, které se ucházejí o členství v EU – v kontextu povinností, které proto musejí naplnit, vytvářejí zákony o ochraně osobních údajů a budují příslušné dozorové instituce.

Výrazem uznání práce Úřadu pro ochranu osobních údajů je nepochybně důvěra, s níž mu Rada Evropy svěřila, aby v Praze v říjnu 2004 zorganizoval a společně s RE uspořádal konferenci. Tématem dvoudenních jednání 14. a 15. října budou „Práva a povinnosti subjektů údajů“. V Praze se tedy na podzim bude na vysokém odborném fóru hovořit o jednom z principů, který je zásadně posilován i novelou českého zákona o ochraně osobních údajů. V obdobném světle pozitivního hodnocení českého Úřadu se jeví i fakt, že jeho předseda byl pozván ministrem vlády Irsku, státu do konce června předsedajícím EU, panem Dermontem Ahernem, aby řídil jeden z panelů květnového summitu EU, který se v Dublinu věnoval problematice biometrie – disciplíny s dynamickou perspektivou vývoje; tímto summitem se biometrie ocitla v agendě problémů, jimiž se na nejvyšší úrovni bude každý z předsedajících států EU v budoucnu opakovaně zabývat. Rovněž přednášky a setkání s vládní administrativou Západního Kapska věnované ochraně osobních údajů, které uskutečnil předseda Úřadu, když byl pozván do Jihoafrické republiky letos v květnu, svědčí o prestiži, které práce českého Úřadu ve světě požívá.

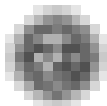
## **Euronovela zákona o ochraně osobních údajů**

*Dnem 26. července 2004 vstoupila v platnost novela zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Publikována je ve Sbírce zákonů pod číslem 439/2004 Sb.*

Návrh zákona byl jako Sněmovní tisk č. 508 Poslaneckou sněmovnou projednán a schválen v dubnu 2004. V květnu byl tento návrh jako Senátní tisk č. 344 přikázán k projednání Výboru pro vzdělávání, vědu, kulturu, lidská práva a petice, který byl určen jako garanční výbor, a dále byl tento návrh projednáván Výborem pro záležitosti EU a Ústavně právním výborem Senátu.

Výsledkem projednávání bylo zjištění, že je nezbytné novelizovat ustanovení zákona o účinnosti a s ním spojená přechodná ustanovení návrhu zákona, neboť se nenaplnilo očekávání navrhovatele, aby zákon nabyl účinnosti dnem vstupu ČR do EU. Současně bylo navrženo doplnění taxativního výčtu citlivých osobních údajů v ustanovení § 4 písm. b) návrhu zákona o tzv. genetická data.

Senát tyto pozměňovací návrhy přijal na své schůzi dne 13. května 2004 a současně tak vrátil návrh zákona zpět Poslanecké sněmovně, která o návrhu rozhodla na své schůzi dne 25. června 2004. Zákon byl dne 14. července podepsán prezidentem republiky. Znění novely tohoto zákona je též přístupné na <http://www.uouu.cz/legisl.php3>.



## Agenda Úřadu ve 2. čtvrtletí roku 2004

Pravidelná čtvrtletní tisková konference Úřadu, která se konala 9. června, bilancovala před přítomnými novináři úkoly, s nimiž se Úřad ve druhém čtvrtletí roku vyrovnával.

Od 11. března 2004 jeho **Odbor legislativní a právní** připomínkoval 93 právních předpisů – z toho 20 zákonů, 42 vyhlášek, 10 nařízení vlády a 21 ostatních předpisů 16 institucí – z toho v největším rozsahu Ministerstva zdravotnictví (29) a Ministerstva životního prostředí (12).

K 7. 6. 2004 je **zaregistrováno** 23 915 zpracování prováděných 21 138 správci osobních údajů.

**Odbor kontroly** za období od 11. 3. 2004 šetřil 35 případů, ukončil 13 případů, 10 případů postoupil inspektorům Úřadu, 1 Ministerstvu zdravotnictví ČR, 1 Magistrátu hl. m. Prahy, 1 ČNB – odboru bankovního dohledu, a 5 předal k řízení Odboru správního rozhodování Úřadu.

V období, které uplynulo od poslední tiskové konference (11. 3. 2004), **inspektorky a inspektoři** Úřadu zahájili 18 kontrol, 21 kontrol ukončili a v 9 pokračují.

V návaznosti na informace, které poskytla minulá tisková konference Úřadu 11. 3. v souvislosti s kauzami, na něž upozornila, nebo kterým se soustředěně věnovala média, lze rekapitulovat následující kroky a postup Úřadu:

V návaznosti na uzavřenou kontrolu v a.s. Tesco Stores ČR a v eBance probíhá správní řízení ve věci porušení zákona.

Ve společnosti SOLUS byla ukončena kontrola a v poslední dekádě května bylo Úřadem zahájeno správní řízení.

Ve společnosti HOMR (Hnutí na ochranu majitelů realit) probíhá kontrola.

V Českých aeroliniích byla ukončena kontrola zaměřená na plnění požadavku Úřadu, aby s touto leteckou společností cestující pasažéři do USA byli dostatečně informováni o předávání svých osobních údajů. Kontrola neshledala porušování požadavku, jímž Úřad podmiňoval předávání osobních údajů pasažérů do Spojených států. Kontrola však měla velmi omezený rozsah.

Předávání osobních údajů leteckých pasažérů do USA bude Úřad nadále věnovat pozornost, mj. i v souvislosti s vývojem postojů EU; Soudní dvůr v Lucembursku má rozhodovat ve věci podání Evropského parlamentu o tom, zda předávání osobních údajů občanů EU cestujících do USA není diskriminační.

**Odbor správního rozhodování** Úřadu obdržel od 11. 3. 2004, od konání poslední tiskové konference, do 8. 6. 2004:

18 nových podnětů k vyřízení (jak přestupků, tak správních deliktů). Z celkového počtu 39 vedených podnětů je 17 řešeno ve správním řízení, 5 je řešeno v řízení o přestupku, 7 podnětů je vyřízeno úředním záznamem, 1 je postoupen orgánu činnému v trestním řízení a 1 podnět je postoupen ke kontrolnímu šetření. Celkem eviduje správní odbor 43 správních řízení, z toho 16 správních řízení bylo zahájeno nově a bylo vydáno 23 rozhodnutí ve věci - z toho 13 rozhodnutí je pravomocných (9 o uložení pokuty, 4 o zastavení řízení), u 4 byl podán rozklad, v 1 rozhodnutí odvolacího orgánu bylo potvrzeno rozhodnutí o uložení pokuty, 10 uložených pokut bylo uhrazeno (v celkové částce 650 000 Kč).

Z 5 podnětů projednávaných podle zákona o přestupcích byly 2 odloženy před zahájením řízení, 1 věc je řešena příkazním řízením - uložena pokuta ve výši 3 000 Kč – příkaz nabyl právní moci; vydáno je 1 rozhodnutí o zastavení řízení (nabylo právní moci), 1 řízení probíhá.

Bližší informaci o trestání deliktů Úřadem, kterému byla věnována speciálně i část tiskové konference 9. 6. 2004, přináší následující příspěvek.

## **Pokutování za porušení povinností při zpracování osobních údajů**

„Správní trestání“, tedy ukládání pokut za prokázaná porušení právních povinností stanovených zákonem o ochraně osobních údajů, je poměrně novým institutem, který kvůli pravidlům platným pro zákonné přechodné období (nutné pro uvedení činností správců a zpracovatelů osobních údajů do souladu se zákonem) bylo možno plně uvést v život až od poloviny roku 2003.

Ukládání pokut je v právním prostředí ČR běžně uplatňovaným nástrojem. V oblasti ochrany osobních údajů tomu tak v některých evropských zemích však není, nebo do nedávné doby nebylo; aplikaci správního trestání nerozvádí ani příslušná směrnice Evropského parlamentu a Rady upravující ochranu osobních údajů, a ponechává tedy kroky v příslušné oblasti fakticky na každém členském státu Evropské unie.

Zákon o ochraně osobních údajů rozlišuje mezi delikty správců a zpracovatelů, tedy subjektů, které vždy nesou odpovědnost za proces zpracování osobních údajů, a přestupky fyzických osob vykonávajících úkoly pro správce nebo zpracovatele. Zatímco přestupky fyzických osob za porušení povinnosti mlčenlivosti či dalších dílčích povinností lze „ocenit“ částkou do 25 000, příp. 50 000 Kč (případ porušení mlčenlivosti), správcům či zpracovatelům osobních údajů, kteří často nakládají s osobními údaji ve velkém rozsahu, lze uložit pokutu do výše 10 mil. Kč, za opakovaná porušení i 20 mil. Kč.

V současné době není dáno konkrétní zákonné vymezení, jakou výši pokuty lze za různá jednotlivá porušení stanovit (rozčlenění výši pokut upravuje s účinností od počátku příštího roku novela zákona o ochraně osobních údajů). Limitem však nemůže být pouze horní hranice sankční sazby, ale vždy je nutno přihlídnout ke všem obecným kritériím stanoveným zákonem o ochraně osobních údajů, kterými jsou povaha, závažnost a způsob jednání, míra zavinění, doba trvání a následky protiprávního jednání.

Z pohledu práva a spravedlnosti nelze v uložení pokuty spatřovat jediný způsob a konečný cíl vyřízení deliktních věcí, neboť smyslem každé dozorové činnosti je náprava závadného stavu, které lze dosahovat v první řadě uložení omezujících, nápravných a případně satisfakčních opatření. V souladu se zákonem je však nutné přistoupit k uložení sankce vždy, pokud je v závažné míře dotčen zákonem chráněný zájem a je tedy zjištěn a popsán nikoliv bagatelní, ale společensky nebezpečný případ porušení zákona.

Úřad pro ochranu osobních údajů je povinen se zabývat každým případem porušení zákona, o němž může získat dostatečně určité informace. O uložení sankce však Úřad rozhoduje v samostatném řízení upraveném správním řádem, příp. přestupkovým zákonem, které zahajuje, v souladu se zákonem, na základě vlastního rozhodnutí. To znamená, že není možno automaticky přistoupit k zahájení řízení o uložení pokuty na základě každého podnětu či stížnosti doručených Úřadu. V mnoha případech dochází k tzv. předběžnému šetření (prověření věci, včetně častého doplnění podnětů a stížností), nebo je vhodné zahájit kontrolu. Již samotné zahájení řízení o uložení pokuty musí být podloženo relevantními poznatky o deliktním jednání.

Úřad pro ochranu osobních údajů se také zabývá případy, které „odložily“ orgány činné v trestním řízení, pokud konstatovaly, že konkrétní skutek, u něhož bylo podezření na trestný čin, je společensky méně nebezpečný a nejedná se tudíž o trestný čin, ale o přestupek. Úřad naopak podává trestní oznámení, pokud na základě zjištěných skutečností dojde k podezření, že by mohl být spáchán trestný čin neoprávněného nakládání s osobními údaji (§ 178 tr. zákona), příp. jiný trestný čin.

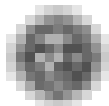
**Úřad pro ochranu osobních údajů:  
Pravomocně rozhodnuté případy ve správním trestání /leden – květen 2004/**

Delikt ní jednání	Sankce	Nápravná opatření
zpracování osobních údajů uchazečů o zaměstnání i citlivých údajů bez výslovného souhlasu subjektů údajů, způsobem zasahujícím do lidské důstojnosti, nedostatečnost opatření proti neoprávněnému zpracování osobních údajů § 9, § 10, § 13	500 000 Kč	ne
formální nedostatečnost souhlasu zákazníků a dalších osob oslovovaných s nabídkou služeb a obchodu § 5 odst. 5, § 11 odst. 1, 2 a 3	40 000 Kč	ano
zveřejnění osobních údajů dlužníků v obecním tištěném periodiku § 5 odst. 1 písm.f)	30 000 Kč	závadný stav napraven
zpracovávání osobních údajů zákazníků a žadatelů o úvěr, uložení v databázi i po skončení důvodnosti zpracování, formální nedostatky souhlasu 5 odst. 1 písm.e), § 5 odst. 5	20 000 Kč	ano
překročení účelu zpracování osobních údajů pacientky zasláním informací o zdravotnickém prostředku § 5 odst. 1 písm. f)	20 000 Kč	ne
zpracování osobních údajů nezletilé osoby při nabídce zboží a služeb bez jejího souhlasu § 5 odst. 2, § 5 odst. 7	20 000 Kč	ano
zveřejnění osobních údajů, včetně citlivých, tří osob na internetových stránkách, v souvislosti se soudními spory § 5 odst. 2, § 10	8 000 Kč	závadný stav napraven
zpřístupnění osobních údajů rozesláním cestovní smlouvy obsahující osobní údaje všech účastníků zájezdu § 5 odst. 1 písm. f)	6 000 Kč	ne
zpřístupnění osobních údajů zaměstnanců smluvním partnerům § 5 odst. 1 písm. f)	5 000 Kč	ano
uvedení osobních údajů dvou osob na vývěsce v domě § 13	1 000 Kč	závadný stav napraven

**Diskusní fórum:**

**Úřad navazuje těsnější kontakty s veřejností**

Kromě pravidelné konzultační činnosti, zodpovídání dotazů i prostřednictvím elektronické pošty a telefonních informačních linek (které fungují prakticky od vzniku Úřadu), poskytl Úřad veřejnosti další možnost klást nejrůznější dotazy, a to na svých internetových stránkách, v podobě Diskusního fóra.



První dotazovací "seance" se uskutečnily 9. dubna a 18. června 2004 v dopoledních hodinách. Byly zaměřeny na způsob využívání rodných čísel po novele zákona č. 133/2000 Sb., o evidenci obyvatel a rodném čísle. Tato novela přinesla Úřadu novou kompetenci postihu neoprávněného nakládání s rodnými čísly občanů. Na příchozí dotazy odpovídali kvalifikovaní odborníci – právníci z řad zaměstnanců Úřadu.

Diskusní fórum bude otevíráno vždy k určitému předem stanovenému tématu, zpravidla k takovému, které je v daném období aktuální. Prozatím se počítá nejméně se čtyřmi seancemi ročně, které budou ohlašovány na pravidelných tiskových konferencích Úřadu.

V budoucnosti nebude Diskusní fórum Úřadu využíváno pouze pro dotazy občanů a organizací. Další možnosti využití fóra spočívají kromě jiného v různých typech on-line besed a kulatých stolů (např. s novináři, odborníky z příbuzných oborů apod.).

Upoutávky s upozorněním na konání dalších diskusních fór budou umístěny na úvodní stránce webu Úřadu a stručná informace bude uveřejněna i v některých hlavních denících.

Zprovoznění Diskusního fóra je dalším krokem na cestě k účinným zpětným vazbám a k užším vztahům Úřadu s veřejností.

*Diskusní fórum je umístěno ve stejnojmenné rubrice na hlavní stránce webu Úřadu pro ochranu osobních údajů ([www.uouu.cz/disk\\_forum.php3](http://www.uouu.cz/disk_forum.php3)).*

## NEMĚLO BY VÁM UNIKNOUT

### Uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky od daně z příjmu

K výše jmenovanému problému, který řeší velké množství občanů, přinášíme výtah z Úřadem vydaného Stanoviska č. 5/2004, jehož plné znění bylo publikováno ve Věstníku č. 32 dne 18. května. Zveřejněno je rovněž na webových stránkách Úřadu ([www.uouu.cz/stan\\_stanoviska.php3](http://www.uouu.cz/stan_stanoviska.php3)).

Daňoví poplatníci – členové odborové organizace – mohou poprvé po skončení roku 2004 uplatňovat pro snížení základu daně z příjmu i členské příspěvky, které zaplatili své odborové organizaci. Umožňuje jim to novela zákona o dani z příjmu.

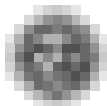
Zákon č. 586/1992 Sb., o daních z příjmu, byl novelizován zákonem č. 438/2003 Sb. Většina nových ustanovení vstoupila v platnost dnem 1. ledna 2004.

Novela je v souladu s cíli ČMKOS, poskytuje odborářům možnost snížení daní. Je ovšem nutné, aby odborová organizace byla schopna vydat svému členovi potvrzení o výši zaplacených členských příspěvků, jak zákon ukládá. Tento postup by neměl činit žádné obtíže organizacím, které samy od svých členů členské příspěvky vybírají. Existuje však nemalý počet odborových organizací, pro které členské příspěvky sráží ze mzdy odborářů zaměstnavatel a poukazuje je na účet odborové organizace. U tohoto způsobu placení členských příspěvků je nutno vážit případnou kolizi se zákonem č. 101/2000 Sb., o ochraně osobních údajů. Samotný problém srážení příspěvků byl řešen ve spolupráci s Úřadem a vyústil ve vydání Stanoviska Úřadu č. 2/2001 „Zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací“, které bylo uveřejněno ve Věstníku Úřadu, částka 12 z 23. října 2001.

V souvislosti s daňovou novelou však problém kolize vyvstává znovu, z jiného úhlu pohledu. Zaměstnavatel sráží členské příspěvky na základě dohody o srážkách ze mzdy uzavřené mezi zaměstnancem a odborovou organizací, která mu byla předložena, a poukazuje tyto příspěvky na účet odborové organizace. Nyní nastávají dle poznatků z praxe dva možné postupy zaměstnavatele:

1. Zaměstnavatel předává každý měsíc odborové organizaci informace formou písemného seznamu s výši srážek u jednotlivých zaměstnanců. Zde nevniká odborové organizaci žádná větší po-





tíž zjistit dle předaných seznamů celkovou roční výši srážek odborových příspěvků a vydat o ní svému členovi potvrzení.

2. Zaměstnavatel převádí na účet odborové organizace pouze celkovou částku sražených odborových příspěvků, bez konkretizace na jednotlivce. V tomto případě musí odborová organizace zjistit, kolik který její člen zaplatil. Existují tři možné varianty postupu. Úřad považuje za elegantní, nejspřehlednější a v zásadě vyhovující požadavkům zákona především následující způsob:

Podle § 5 odst. 2 písm. a) citovaného zákona může správce zpracovávat osobní údaje i bez souhlasu subjektu údajů, jestliže provádí zpracování stanovené zvláštním zákonem nebo nutně pro plnění povinností stanovených zvláštním zákonem. Je přitom pouze povinen, podle odst. 3 téhož ustanovení, dbát práva na ochranu soukromého a osobního života subjektu údajů. Tímto zvláštním zákonem je právě zákon o dani z příjmu, který umožňuje odečíst zaplacené členské příspěvky od základu daně a zároveň ukládá povinnost předložit o tom potvrzení. Jestliže srážky provádí zaměstnavatel a ke zjištění jejich výše, pokud jde o odborářské příspěvky, je nutně pro plnění povinností odborové organizace vydat o jejich výši daňovému poplatníku potvrzení, pak je v souladu se zákonem o ochraně osobních údajů, když zaměstnavatel odborové organizaci poskytne roční přehled o zaplacených příspěvcích od jednotlivých daňových poplatníků. Důležitá je také skutečnost, že v souladu se zákonem o dani z příjmu nemusí zaměstnavatel v souvislosti s tímto sdělením oznamovat Úřadu, že hodlá zpracovávat citlivý osobní údaj. Poté, co zaměstnanec má v ruce potvrzení odborové organizace o výši členských příspěvků, které za zdaňovací období zaplatil, podává daňové přiznání sám nebo, jestliže tuto povinnost nemá, zúčtování daňových záloh provádí jeho zaměstnavatel.

Výše možné odečitatelné částky z daní je určena dvěma limity. První limit je stanoven do výše 1,5 % zdaniitelných příjmů, druhým limitem je maximální částka 3000 Kč za zdaňovací období. Pro uplatnění nároku na uznání odpočtu je potřeba, aby zaměstnanec (člen odborového svazu) předložil zaměstnavateli potvrzení odborové organizace o výši zaplaceného členského příspěvku v zákonné lhůtě a na předtištěném formuláři.

Detailní rozbor problematiky viz Věstník Úřadu pro ochranu osobních údajů, částka 32 z 18. května 2004, nebo na adrese [www.uoou.cz/stan\\_stanoviska.php3](http://www.uoou.cz/stan_stanoviska.php3)

## TÉMA – KAMEROVÉ SYSTÉMY

### Vidí vás ...

*Obrazovka současně přijímala a vysílala. Každý zvuk, který Winston vydal a jenž byl hlasitější než velmi tiché šeptání, obrazovka zachycovala, a co víc, pokud zůstával stát v zorném poli kovové desky, bylo ho vidět a slyšet. Samozřejmě, člověk si nikdy nebyl jist, zda ho v daném okamžiku sledují.*

*George Orwell: „1984“*

Pohyb na mnoha veřejných prostranstvích nepřetržitě sledují stovky kamer policie i soukromých firem. V Česku neustále přibývá počet kamerových systémů, které dění na ulicích zaznamenávají. Víte kolik bezpečnostních kamer je například umístěno na půlkilometrové ulici Na Příkopě v centru Prahy? Pravděpodobně málokdo z nás by odpověděl správně – údajně jedenadvacet! Naše země se dostává na úroveň západoevropských států, kde je monitorování veřejných prostranství běžnou záležitostí. Většina z nás má přirozené obavy, jistou nedůvěru a pocit umenšení osobních svobod. Kamera je jednoznačně klasickým „orwellovským“ nástrojem, který sleduje naše chování v reálném čase.

Na druhé straně je nutně zdůraznit, že kamerové systémy slouží k boji s narůstající kriminalitou, k odhalování trestné činnosti, k její prevenci a napomáhají zajistit bezpečnost osob i majetku. Instalace kamerových systémů je účinným pomocníkem při ochraně veřejného pořádku i při obraně



státu. Kamerové systémy umístěné na úřadech mohou, podle zkušeností, přispět ke zklidnění mnohdy vypjaté atmosféry mezi klienty a zaměstnanci a v případě nepříznivého vyústění konfliktní situace má tak dotyčný úřad k dispozici objektivní záznam.

Odborníci však varují, že záznamy z kamer jsou zneužitelné a je zřejmé, že zákonná úprava, která by používání kamer regulovala, je nedostatečná. Příklady zneužití záznamů se objevily již i u nás (například ochranka v jednom ze supermarketů pomocí kamerového systému natáčela zákaznice v převlékacích kabinkách, nebo se záznam s chováním posádky vozu, natočený městskou policií, následně dostal na veřejnost). Stížnosti se také objevují na užití kamer u obytných domů. Správce systému má díky kamerám přehled, kdy který z nájemníků přichází domů a kdy odchází (eventuálně s kým). Hrozí ale také, že se informace o tom, který byt je právě prázdný, dostane k někomu dalšímu.

Kamerové systémy začali také užívat mnozí zaměstnavatelé k monitorování svých zaměstnanců v zaměstnání.

Je nutno říci, že záznamy z kamerových sledovacích systémů, pokud obsahují tváře či jiné identifikační znaky osob, podléhají režimu zákona o ochraně osobních údajů. Na shromažďování a zpracování informací z takových systémů se tedy vztahují všechny principy této ochrany podle zákona o ochraně osobních údajů, případně jiných právních předpisů o ochraně soukromí jednotlivců.

Při ochraně soukromí lze ovšem také vycházet z Listiny základních práv a svobod čl. 10 o zachování lidské důstojnosti a ochraně před neoprávněným zasahováním do soukromého a osobního života, z ustanovení zákoníku práce § 7 odst. 2, podle něhož nesmí být mimo jiné zásah do práv zaměstnanců v rozporu s dobrými mravy, a z občanského zákoníku § 11 až 13.

Lze konstatovat, že do jisté míry je v ČR na užívání kamer možné aplikovat zákon o ochraně osobních údajů, kde je uvedeno, že správce osobních údajů musí jasně stanovit účel jejich shromažďování (zpracování). Důležité je mít na zřeteli, že uchovávané záznamy kamer mohou obsahovat osobní údaje a jako s takovými je s nimi nutno nakládat. Pokud by je někdo zneužil, může být podle zákona o ochraně osobních údajů sankcionován.

Jako každý „výdobytek lidského rozumu a umu“ má svůj rub i líc, tak i průmyslová kamera umístěná na správném místě a řádně používaná podle pevně stanovených pravidel je pro společnost přínosem. V případě, že nejsou taková pravidla dána či nejsou řádně dodržována, může docházet k nepříjemným situacím nebo ke zneužití záznamů.

Veřejnost by si měla na užívání sledovacích kamer, instalovaných na předem určených a označených místech v rámci ochrany bezpečí, zvyknout. Je to přirozený vývoj, který by ovšem měl mít jasná pravidla.

Naše soukromí a identita je i naší svobodou, kterou musíme hájit, ale kterou si musíme také zasloužit. Třeba tím, že budeme racionálně a zodpovědně přistupovat ke všem objevům vědy a techniky, k možnostem, které nabízejí nové technologie. Neměli bychom zapomínat...

*Předpokládalo se, že sledují každého neustále. A rozhodně mohli zapnout vaše zařízení, kdy se jim chtělo. Člověk musel žít – a žil, ze zvyku, který se stal pudovým v předpokladu, že každý zvuk, který vydá, je zaslechnut, a každý pohyb, pokud není tma, zaznamenán.*

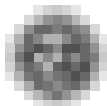
*Goerge Orwell: „1984“*

## K věci:

### Italský dozorový orgán ochrany dat vydal pokyny pro kamerové sledování

20. května t.r. vydal Úřad pro ochranu osobních údajů (Garante per la protezione dei dati personali) v Itálii pokyny týkající se instalace sledovacích kamer. Upozorňuje především, že důležité je nejprve posoudit, zda instalování tohoto zařízení na daném místě skutečně splní zamýšlený účel a zda by ne-





bylo dostačující využití jiných druhů zabezpečení (např. alarm). Pokud obrazový materiál nasnímaný kamerou umožňuje identifikaci jednotlivých osob, smí být kamera umístěna pouze tam, kde by účelu snímání nebylo dosaženo shromažďováním anonymních dat. Lidé pohybující se v dosahu kamery musejí být o tomto faktu informováni, stejně jako o tom, kým byla kamera instalována a proč. Nevýžaduje-li výjimečnost situace uložení nahrávky po delší dobu, smí být uchovávána max. 24 hodin, u některých institucí (banky atp.) maximálně 1 týden. V každém případě by měly být pro uchovávání nahrávek stanoveny přísné podmínky, a pokud je to dostačující, měly by se používat spíše kamery pro sledování, nikoliv také pro nahrávání.

Veřejné instituce smějí provádět kamerové sledování pouze tehdy, je-li to nezbytné pro řádný výkon jejich funkce (soudy, policie, atd.). V nemocnicích je využití kamery povoleno jen na určitých odděleních, ve školách, pouze pokud je to nezbytně nutné, a to jen mimo dobu vyučovacích hodin. Přítomnost kamery ve veřejných dopravních prostředcích, v církevních objektech nebo na hřbitovech může být povolena pouze za určitých podmínek. Zcela zakázáno je snímání větších prostranství ve městech, stejně jako kamerové sledování malých přestupků (porušení zákazu kouření, vstupu na trávník atp.). „Absolutně zakázáno“ je také sledování zaměstnanců jejich zaměstnavateli.

Kamerové sledování k soukromým účelům musí buď vyplývat ze zákona, nebo musí sloužit k zajištění ochrany osob a majetku proti násilí, krádežím, vandalizmu, vloupání, požáru atp. Majitel soukromého objektu musí vždy zaručit, že kamera zabírá výlučně jen jeho vlastní majetek a nikoliv části veřejného prostranství.

*Zpracováno podle informací v angličtině na:*

*<http://www.statewatch.org/news/2004/may/19italy-surveillance.htm>*

*Celý text v italštině lze najít na:*

*<http://www.cittadinolex.kataweb.it/Article/0,1519,2864314,00.html>*

## **Švýcarské zkušenosti:**

### **Videokamery proti vandalizmu**

V posledních letech jsme v ČR častými svědky rostoucího vandalizmu na železnicích, ať už jde o lidské životy ohrožující krádeže materiálu na vlakových tratích, o pobuřující až agresivní chování některých fanoušků při jejich cestách za fotbalovými zápasy nebo například o mnohdy se pokusy o bombové atentáty. Při cestování vlakem se bohužel vykradené vybavení tratí, akty násilí na cestujících a zdevastované interiéry vlakových souprav staly běžným jevem. Tento stav je naprosto nespokojivý nejenom z hlediska železničních společností a jejich dobré pověsti, ale především z hlediska ohrožené bezpečnosti pasažérů.

Podobné problémy se však zřejmě vyskytují i v jiných zemích. Ve Švýcarsku se rozhodli čelit (alespoň částečně) těmto problémům instalací videokamer, prozatím pouze na některých vybraných regionálních vlakových linkách. Vedení železniční společnosti CFF vydalo pokyn k vybavení vlakových souprav na těchto tratích sledovacími videokamerami.

Tento krok však vyvolal řadu otázek, které se týkaly zejména dalšího nakládání s pořízenými video záznamy a případných kolizí se zákony o ochraně osobnosti, soukromí a osobních údajů. Po dohodě vedení železniční společnosti se švýcarským spolkovým úřadem pro ochranu dat byla stanovena tato základní pravidla pro videodohled ve vlakových soupravách:

- Cestující budou upozorněni na přítomnost videokamer prostřednictvím dobře viditelného a čitelného štítku umístěného na vagónech.
- Videozáznamy nebudou prohlíženy průběžně: Budou zapisovány na pevné disky a v případě, že do 24 hodin nebude podána žádná zpráva o nějaké mimořádné události ve sledovaných prostorech, budou po uplynutí této lhůty smazány.
- V případě, že dojde k problémům, bude k prohlížení a vyhodnocování záznamů oprávněna pouze železniční policie ve spolupráci s kantonálními policejními složkami.



Ze závěrů studie, kterou si nechala zpracovat společnost CFF v průběhu testů realizovaných na trati Lausanne – Payerne vyplývá, že zavedení kamer na železnicích posiluje v pasažérech pocit bezpečnosti a může snížit řádění vandalů až o 80 %.

Pro země, které se každodenně potýkají s rostoucím vandalstvím a s násilnostmi na železnicích, může být švýcarská zkušenost zajímavá.

## Kamerový dohled realizovaný soukromými osobami

Používání videokamer soukromými osobami za účelem ostrahy v situacích, kdy se pořízené filmy vztahují na jednu nebo více identifikovaných nebo identifikovatelných osob (bez ohledu na to, zda je na filmovaný materiál dále uchováván či nikoli), je ve Švýcarsku upraveno spolkovým zákonem o ochraně dat z roku 1992. Zpracování takto získaných materiálů (výběr jednotlivých snímků, přenos, průběžné nebo následné prohlížení filmů, jejich zálohování a uchovávání apod.) musí podléhat všeobecným zásadám ochrany dat.

V tomto příspěvku se hovoří o kamerovém dohledu, který provádějí soukromé osoby v soukromých prostorách (ať už přístupných či nepřístupných veřejnosti). Nebude zde pojednáváno o kamerovém dohledu na pracovištích.

Provoz systémů kamerového dohledu je možný pouze tehdy, jsou-li splněny dvě základní podmínky:

1. Kamerový dohled může být realizován pouze se souhlasem a s vědomím dotyčných osob, zdůvodněným veřejným či soukromým zájmem nebo příslušným zákonem. (Princip legality)

Příklad: Majitel klenotnictví má svrchovaný zájem na tom, aby jeho obchod nebyl během jeho nepřítomnosti vyloupen.

2. Kamerový dohled musí být přiměřeným prostředkem, nutným k zajištění bezpečnosti předmětů ostrahy, tedy především jednotlivých osob a/nebo objektů. Měl by být využíván pouze tehdy, nejsou-li realizovatelné, dostatečně účinné či postačující ostatní bezpečnostní prostředky a nástroje (jako například přídavné bezpečnostní zámky, zesílení pevnosti vstupních dveří či bran, výstražné systémy apod.). (Princip přiměřenosti)

Příklad: Instalace videokamer v prostorách skladiště je v zásadě přijatelná, zejména jako prostředek k ochraně proti vandalismu a krádežím.

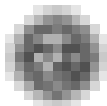
Pro instalaci a využívání systémů kamerového dohledu je třeba dodržovat následující pravidla:

1. Osoba odpovědná za kamerový systém je povinna informovat jednotlivce, kteří vstupují do záběru videokamery, o přítomnosti takového systému, a to dobře viditelným a čitelným upozorněním. Jsou-li výstupní data z kamer dále shromažďována a případně vázána k dalším údajům, upozornění musí obsahovat údaj o kontaktu na osobu, na níž se v případě potřeby přístupu k příslušným údajům může sledovaný jedinec obrátit. (Princip důvěry a práva přístupu)

Příklad: Přítomnost sledovací videokamery, umístěné při vchodu do obytného domu, musí být oznámena dobře viditelným nápisem všem jednotlivcům, kteří do budovy vstupují.

2. Osoba odpovědná za kamerový systém je povinna učinit všechna nezbytná technická a organizační opatření k tomu, aby dotyčným jednotlivcům byla zajištěna ochrana jejich osobních údajů před nepovoleným zpracováním a před dalším možným zneužitím těchto údajů. (Princip bezpečnost dat)

Příklad: K monitorům zobrazujícím kamerové záznamy mohou mít přístup pouze k tomu povolané osoby. Nahrané videozáznamy musejí být uloženy a uchovávány na bezpečném a uzamčeném místě. Klíč k tomuto místu smí být přístupný pouze oprávněným osobám.



3. Sledovací kamera musí být umístěna tak, aby zorné pole jejího objektivu zobrazovalo pouze záběry nezbytně nutné pro stanovený účel sledování. (Princip přiměřenosti)

Příklad: Sledovací kamera umístěná v obytném domě nesmí umožňovat obrazovou informaci o tom, která osoba vstupuje do určitého bytu.

4. Data – výstupy z videokamer – nesmějí být využívána za jiným účelem než v rámci ochrany osob a majetku. (Princip účelu)

Příklad: Snímky pořízené videokamerou, která byla v sídle obchodní společnosti nainstalována z bezpečnostních důvodů, nemohou být využívány například k propagačním či marketingovým účelům.

5. Předávání videozáznamů prozrazujících totožnost osob je možné pouze v případech předvídaných nebo povolených zákonem, např. na základě soudního příkazu. (Princip účelu)

Příklad: Videozáznamy pořízené sledovací kamerou nesmějí být předávány nebo prodávány třetí straně.

6. Videozáznamy z kamer musejí být v krátké lhůtě vymazány. Ke zjištění škody na majetku či na osobách totiž v naprosté většině případů dochází v intervalu nejvýše několika hodin po vzniku této škody. Zdá se tedy, že čtyřadvacetihodinová lhůta pro uchování záznamu je v takových případech zcela postačující. V případech kamerové ostrahy soukromých míst, která nejsou přístupna veřejnosti, může být tato lhůta delší. (Princip přiměřenosti)

Příklad: Nepřítomnost majitele střeženého objektu, například z důvodu jeho dovolené, může ospravedlňovat delší lhůtu pro uchování videozáznamu. Nedošlo-li však během tohoto období k žádné mimořádné události, záznam by měl být co nejdříve po návratu majitele smazán.

Zdroj: Internetové stránky švýcarského Úřadu pro ochranu dat:  
[www.edsb.ch/f/doku/merkblaetter/video.htm](http://www.edsb.ch/f/doku/merkblaetter/video.htm)

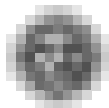
## Enormní nárůst kamerových sledovacích systémů ve Velké Británii

Britové jsou „nejsledovanějším národem“ na zeměkouli. Vyplývá to ze zprávy přednesené v lednu 2004 na konferenci pořádané na univerzitě v Sheffieldu, kde bylo uvedeno, že podle posledního průzkumu vzrostl za poslední tři roky počet sledovacích kamer čtyřnásobně. V praxi to znamená, že v současné době ve Velké Británii monitorují ulice, budovy a osoby 4 miliony kamerových sledovacích systémů. Tento enormní nárůst je „darem“ pro výrobce těchto zařízení, bohlavem pro ochranu soukromí a prostorem pro neshodu mezi občany. Otázka zní, zda se nyní občané cítí výrazně bezpečněji, nebo zda se cítí výrazně méně bezpečně a mají pocit menší svobody.

## Férovost vůči lidem

### Rozhovor s RNDr. Karlem Neuwirtem, předsedou Úřadu

*Pane předsedo, v tomto čísle věnuje bulletin Úřadu pozornost tématu využívání kamerových systémů. Zmíněna je mimo jiné i situace ve Velké Británii. Vy jste se zúčastnil semináře v této zemi a v Manchesteru jste viděl, jak jsou kamery v nemalém rozsahu používány. Obcházel Vás při tom nějaký orwellovský přízrak, nebo naopak jste měl dojem, že lze docílit toho, aby převládala pozitivní stránka využívání kamer pro život občanů? A co je k eventuální převaze pozitiv ve využívání kamer potřeba?*



V Manchesteru jsem byl na pracovním semináři; policie na něm prezentovala kamerový monitorovací systém. Bylo to velmi zajímavé, Manchester je zřejmě i pro Británii jakési modelové místo.

Ale orwellovský přízrak mne ani tak neobcházal v ulicích Manchesteru, protože kameru zaznamenáte jenom tu a tam, někdy je navíc i poměrně daleko od vás. Zato ve „velině“, který jsme také navštívili, kde je na jedné stěně instalováno asi 50 monitorů, každý rozdělený minimálně na 4 pole a vidíte, jak jde mezi kamerami přepínat, do jakých detailů lze zaostřovat – tam ten „syndrom Velkého bratra“ na mě výhrůžně dýchl. Jenomže obraz na monitorech sledují civilisté a jenom jediný přítomný řídicí policejní důstojník může dát příkaz, aby se začalo nahrávat – a to jen v případě, kdy je zaznamenáno něco, co vzbudí podezření, třeba náznak násilného nebo trestného činu.

Ten velmi nepříjemný pocit, že kamkoliv se pohnete, může vás sledovat kamera, vyvažuje zjištění, že v Manchesteru na sledovaných místech najdete tabulky, které vás informují, že prostor je monitorován kamerou, a najdete na nich i odkaz, včetně telefonu, kam se můžete obrátit, abyste získal bližší informace o sledování.

Kamery jsou instalovány nejen na ulicích, ale v mnoha veřejných prostorách, například v garážích, na parkovištích... V Londýně se také monitorují poznávací značky automobilů. A když potom slyšíte, jak se díky umístění kamer například snížila kriminalita nebo trestná činnost jako jsou krádeže nebo násilná přepadení a tak dále, potom začnete pokládat na misku vah pocit ohrožení soukromí a na druhou přínos pro občany. Lidé obvykle více slyší na argumentaci větší bezpečnosti ve městě a snížení kriminality a tu možnost ztráty soukromí si ani neuvědomují.

Je třeba také říci, že v Manchesteru je dodržování právních norem naprostou samozřejmostí. To znamená, že jsou skutečně stanovena pravidla, kdo smí pořizovat záznam, za jakých okolností, jak může být využit, jak dlouho se smí uchovávat a podobně.

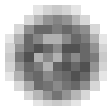
### ***Kdybyste porovnal své poznatky z Velké Británie se situací v České republice, co byste řekl, jaké zásady by měly být uplatněny ve stávajícím právním prostředí v ČR?***

V České republice zatím chybí ustanovení, podle kterých by se měl řídit každý, kdo chce průmyslovou kameru užívat. Úřad pro ochranu osobních údajů chce tuto situaci do budoucna změnit. Nemá však zákonodárnou iniciativu. Uvítal by ovšem, a bude o to usilovat, aby v příští novele zákona o policii bylo stanoveno, jak se má se záznamy z kamer nakládat. V Británii se například nahrávka maže do třiceti dnů a jedině v případě, že je použita jako důkazní materiál v soudním sporu, je uchovávána třicet let.

Samozřejmě je nutno stanovit, zda kamery mají být opravdu jenom sledovací, to znamená, že se nic nenahrává, že se jenom sleduje na obrazovce, co se děje v ulicích města apod. Proces monitorování nesmí záviset na libovůli zřízence nebo úředníka, který sedí před obrazovkou a něco si nahraje, kdy ho to napadne. Dobře víme, že už i u nás došlo ke konfliktním situacím, kdy záznam byl používán úplně k jinému – dokonce zábavnému – účelu, než k němuž byl určen. Občané by měli vědět, že je snímá kamera, že vůbec bude záznam pořizován, zda bude archivován, kdo ho bude vyhodnocovat a podobně. Role ochránců soukromí spočívá v tom, aby dohlíželi na to, že monitorovací systémy budou používány čestným, férovým a legitimním způsobem, aby tyto systémy nebyly propojovány se systémy jinými, aby prioritně sledování bylo anonymní, a teprve při detekci nějaké deliktní činnosti se sledovala konkrétní osoba, nebo konkrétní poznávací značka vozidla, eventuálně aby docházelo k rozpoznávání tváří a podob občanů. Z hlediska ochrany osobních údajů správcům, uživatelům monitorovacích systémů lze klást také otázku, zda by téhož efektu, jehož chtějí pomocí sledování kamerou dosáhnout nebylo možné docílit jinými způsoby. Aby ti, kteří mají zájem instalovat tyto systémy museli mít dostatečné argumenty, proč ano, proč je to nezbytné, že není jiné cesty a že je to vlastně pro ochranu lidí.

Je třeba mít vždycky na zřeteli tak zvaný balanční princip: Chránit občany, zajistit jim bezpečnost a na druhé straně chránit také jejich soukromí.

Toto si myslím že je jakýmsi základním východiskem, aby se udržel přiměřený rámec monitorování a sledování osob ve veřejném prostoru.



## CO NOVÉHO V ZAHRANIČÍ

### Zavádění národních identifikačních průkazů ve Velké Británii

Po více než padesáti letech si pravděpodobně budou muset Britové opět zvykat na identifikační průkazy.

Britský ministr vnitra David Blunkett uveřejnil 26. dubna návrh zákona o národních identifikačních průkazech (ID) a slíbil, že tyto průkazy mají být zárukou svobod, a nikoli jejich ohrožením. Návrh zákona si klade za cíl zavedení biometrických prvků v průkazech, které by měly být povinné od roku 2013 a měla by být vybudována i národní databáze. Přestože ministr vnitra prohlásil, že veřejnost chápe a podporuje nezbytnost zavedení těchto karet, objevují se i kritické hlasy. Odborníci na problematiku terorismu upozorňují, že zavedení nových ID bude mít nepatrný vliv na zvýšení ochrany vůči teroristickým akcím a ochránci lidských práv upozorňují na možné omyly a chyby i na nebezpečí zneužití dat.

Dnem 26. 4. byl současně odstartován zkušební provoz celého systému. Deset tisíc dobrovolníků dostalo nové ID průkazy, aby se vyzkoušela jejich funkčnost a praktičnost. Časem by měly být nové identifikační průkazy povinné pro všechny. Zákon bude parlamentu předložen letos na podzim. První biometrické pasy by měly být vydány v roce 2005 a první karty nesoucí otisky prstu v roce 2007. Podle Davida Blunketta by do roku 2013 mělo mít biometrickou identifikaci 80 % obyvatel buď ve formě pasu, řidičského průkazu nebo dobrovolného identifikačního průkazu.

### Belgie vytvořila „nepadělatelný“ pas

Belgické pasy byly opakovaně předmětem kritiky, že jejich padělky a kradené exempláře doslova zaplavují „světový trh“ s ilegálními cestovními dokumenty. Belgické ministerstvo zahraničí přišlo se zcela novým typem pasu, jehož padělání je prý téměř nemožné.

V posledních letech se množily případy, kdy nejrůznější zločinci použili padělaných belgických pasů. Také jeden z podezřelých ze spáchání nedávného bombového atentátu v Madridu byl držitelem takového dokumentu.

Belgie se proto rozhodla vytvořit nový pas a výsledek svého snažení prezentovala v Bruselu dne 17. května 2004 prostřednictvím Ministerstva zahraničních věcí. Dokument je opatřen speciálním mikročipem, který obsahuje biometrické informace o jeho držiteli. Těmito informacemi mohou být otisk prstu, obraz duhovky nebo podrobné údaje charakterizující obličej. Tvůrci tohoto dokumentu jsou přesvědčeni, že jeho padělání bude téměř vyloučeno, poněvadž každý exemplář má přímou vazbu na svého držitele.

Počínaje příštím rokem chce Belgie začít vydávat nové pasy občanům. Tento krok je v souladu s iniciativou Evropské unie, která si klade za cíl zavést moderní, vysoce zabezpečené cestovní dokumenty do roku 2005.

Ozývají se však i kritické hlasy. Mnoho organizací, zabývajících se občanskými svobodami, se obává pokusů vlád o systematické shromažďování příliš velkého počtu osobních údajů o jednotlivcích.

*Volně zpracováno podle článku umístěného na internetové adrese:  
[www.expatica.com/](http://www.expatica.com/) (internetový zdroj zpráv a informací v anglickém jazyce)*

### Portugalsko dočasně obnovilo kontroly na hranicích

Fotbaloví fandové i ostatní návštěvníci se při cestě do Portugalska museli podrobit pohraniční kontrole. Toto opatření bylo zavedeno pro posílení bezpečnosti v souvislosti s mistrovstvím Evropy ve fotbale a trvalo až do skončení tohoto fotbalového svátku.



Přechodné obnovení kontrol na vnitřních „schengenských hranicích“ jedné země je v souladu s chystaným nařízením ustavujícím Kodex Společenství (Community Code) o pohybu osob přes hranice, jehož návrh Evropská komise předložila dne 26. května 2004.

Tento kodex má dvě části. První se věnuje vnějším hranicím, druhá vnitřním, tj. hranicím mezi jednotlivými státy schengenského prostoru. A právě tato druhá část upravuje různé procedury dočasného opětovného zavedení hraničních kontrol v případě ohrožení například veřejného pořádku, národní bezpečnosti nebo zdraví obyvatelstva určitého členského státu. Byl také zaveden nový postup k obnovení hraničních kontrol na všech, nebo jen některých vnitřních hranicích pro případ výjimečně závažného ohrožení, zejména mezinárodní teroristické hrozby.

Důvodem k předložení výše uvedeného návrhu nebylo ovšem jen vyjasnění nebo zavedení příslušných mechanismů. Cílem předkladatele bylo vyjasnit, restrukturalizovat a dále rozvinout stávající legislativu týkající se hraničních kontrol osob. Návrh vychází z tzv. schengenského mezivládního rámce a má posunout agendu hraničních kontrol více do oblasti kompetencí EU. Přijetí tohoto dokumentu bude vyžadovat jednohlasnou podporu členských států.

### **Sedm let vězení za spam**

Ve Spojených státech vynesl soud precedenční rozsudek, kterým poprvé poslal rozesílatele nevyžádaných elektronických sdělení (spam) do vězení, a to na sedm let.

Howard Carmack dokázal během jednoho roku odeslat pod falešným jménem téměř 850 milionů e-mailů. Přitom použil 343 různých e-mailových kont, které odcizil jejich majitelům. V květnu 2003 byl nakonec zatčen. Obžaloba ho, mimo jiné, obvinila z krádeže identity. Celkem byl shledán vinným ve čtrnácti případech. Soud v Buffalu ho nakonec odsoudil k nejvyššímu trestu, sedmi letům vězení. Proslýchá se ovšem, že při dobré obhajobě by se byl mohl vyhnout tak vysokému trestu.

Ještě před tímto rozsudkem podal proti Carmackovi žalobu také poskytovatel internetového připojení Earthlink, sídlící v Atlantě. Zněla na 16,4 milionů dolarů a byla úspěšná.

Předpokládá se, že tento přísný trest bude mít odstrašující účinek na další spammery.

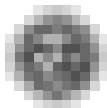
*Volně zpracováno podle německého časopisu  
Manager Magazin ([www.manager-magazin.de](http://www.manager-magazin.de))*

### **Otevření programů na pomoc obětem krádeže identity v USA**

Společnosti Citigroup a Washington Mutual zahájily programy na pomoc zákazníkům, kteří se stali oběťmi krádeží identity, a jejichž jména a čísla účtů byla zneužita. V červnu také národní organizace reprezentující banky, makléřské firmy a finanční společnosti otevře centrum – Theft Assistance Center – za účelem pomoci takto postiženým občanům. „Krádež identity dosáhla v USA rozměrů epidemie“, prohlásil představitel Financial Services Roundtable.

Obě výše uvedené společnosti nabízejí zdarma poradenské služby zákazníkům postižených krádeží identity a také možnost pojištění. Centrum pomoci bude zájemcům poskytovat nejenom pomoc a radu, ale bude také vytvářet databáze, které v případě potřeby mohou být nabídnuty i organizacím činným v oblasti výkonu práva.





## OSOBNÍ ÚDAJE V ŠIRŠÍCH SOUVISLOSTECH

### Evropský ochránce dat v polském Sejmu

První evropský ochránce osobních dat Peter Hustinx, který byl do funkce jmenován 22. prosince 2003, navštívil letos v květnu Polsko. Do Polska jej pozvala paní dr. Ewa Kulesza, generální komisařka ochrany dat Polska. Při této příležitosti přednesl v Sejmu závažný projev.

Polský parlament tak využil příležitosti poznat zásady evropského reprezentanta ochránců dat, který bude sledovat a ovlivňovat celkovou kulturu ochrany dat v EU. K aktuálním otázkám, k nimž se pan Hustinx – dříve dlouholetý šéf nizozemského úřadu pro ochranu osobních údajů – vyjádřil, bylo nastolení rovnováhy mezi respektováním základních práv a svobod a přijímanými opatřeními na zvýšení bezpečnosti a s tím související problém předávání osobních údajů leteckých pasažérů do USA. Hustinx nepovažuje tento problém za uspokojivě a dostatečně vyřešený nedávnou dohodou EU-USA. Prezentoval také názor na vztah mezi ochranou osobních údajů a přístupem veřejnosti k dokumentům ES (tedy svým způsobem reflektoval problém, jaký občas vyvstává u nás při hledání vyváženého vztahu mezi zákonem o ochraně osobních údajů a zákonem o právu na přístup k informacím).

Celý projev, který zazněl v polském Sejmu, je dostupný na nově zřízených webových stránkách evropského ochránce osobních údajů: [www.edps.eu.int](http://www.edps.eu.int).

## Dnes a dříve

### Trestný čin: odboj právu

*Zákon o ochraně osobních údajů, pokud bychom měli věřit některým výrokům, často též denního tisku, zabráňuje 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.*

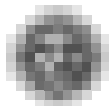
*Pro nás jsou důležitější formální pravidla. Byla velmi podrobná. Posel kupříkladu nesměl být ozbrojen a musel se vykázat velkou pečeti zemského soudu s vyobrazením svatého Václava. K předání dokumentu muselo dojít ve všední den, a to ještě dopoledne.*

*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.*

*Pojdme již ale 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 chvíli čekání se přichozích 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 neboží státní úředníci bez jakéhokoli vysvětlení zůstali až do dalšího rána.*

*Teprve tehdy s nimi kdosi začal komunikovat. Byli to povězní, 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 doručované písemnosti.*

*Na žádné pečlivé pročtení, jak by se dalo očekávat, už ale nedošlo. Krumlovský pán totiž listiny i s pečeti vzápětí rozřezal na několik kusů. Na to užaslého posla vyzval k jejich konzumaci. Ten sice okamžik váhal, hrozící kyj v ruce 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 Tomáš 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 ze zámku.*

*Tím náš příběh vlastně 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.*

*J.M.*

VYDAVÁ ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

EDITOR: PHDR. HANA ŠTĚPÁNKOVÁ

REDAKTOR: MILENA NEJEDLÁ, BOHUMÍR LUKAJ

ADRESA REDAKCE: ÚOOÚ, PPLK. SOCHORA 27, PRAHA 7, 170 00

TELEFON: 234 665 286, FAX: 234 665 505

E – MAIL: INFO@UOOU.CZ

INTERNETOVÁ ADRESA: WWW.UOOU.CZ

PERIODIKUM JE ZAPSÁNO V EVIDENCI PERIODICKÉHO TISKU POD ČÍSLEM MK ČR E 10548

© ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ 2004

DÁNO DO TISKU 26. 7. 2004