# DOKTORANDSKÉ PŘÍSPĚVKY

## Informace v režimu zvýšené ochrany právem Evropské unie: citlivé údaje

Daniel Novák*

### *1. Legální vymezení pojmu „citlivý údaj“*

Podle čl. 8 odst. 1 Směrnice Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (Data Protection Directive, dále jen „DPD“) členské státy zakáží zpracování osobních údajů, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního života.[1]

Obecné pravidlo tedy stanoví, že zpracování citlivých údajů je zakázáno; odchylná řešení představují

* Mgr. Daniel Novák, Ústavní soud ČR.

[1] Srov. čl. 6 belgického zákona, § 7 dánského zákona, francouzský zákon č. 78–17 v čl. 8, v rozhodných souvislostech jsou významná ustanovení § 3 odst. 9, § 4d odst. 5 a § 28 odst. 6 německého spolkového zákona a § 13 švédského zákona.

výjimku, se kterou se spojuje požadavek restriktivního výkladu.

Samotný koncept citlivých údajů není přijímán bez výhrad. Lidskoprávní katalogy nezakotvují výslovně kategorii citlivých nebo speciálních údajů; s výjimkou Listiny základních práv Evropské unie však neupravují explicitně ani ochranu osobních údajů, ale pracují s obecnějším pojmem soukromí. Britský Komisař pro informace konstatoval, že koncept citlivých údajů vychází z chybného předpokladu, neboť citlivost údajů je dána jejich kontextem, nikoli obsahem. Zákon z roku 1984 tuto speciální kategorii neobsahoval a na újmu práv občanů to nebylo.[2]

Zpochybňování je představitelné rovněž co do výběru citlivých údajů dle hledisek blízkých antidiskriminačnímu právu, které není obecně uznáváno. O další posílení charakteristiky se v roce 2002 pokusily Finsko, Rakousko, Spojené království a Švédsko návrhem na přeformulování zákazu zpracování citlivých údajů na zákaz zpracování údajů, které zahrnuje jakýkoli druh diskriminační praxe.[3]

Naopak kupříkladu údaje ekonomické povahy – mnohdy pro jednotlivce významnější – stojí mimo dosah této úpravy. Pouze některé členské státy stanovily zvláštní omezení též pro zpracování údajů ohledně schopnosti splácet úvěry (kupř. Dánsko, Finsko, Nizozemsko, Portugalsko a Řecko).

Dalším problematickým opomenutím, souvisejícím s menším rozšířením technologií způsobilých zjistit pozici jednotlivce v době přípravy DPD (GPS, mobilní telefony, Wi-Fi sítě, RFID apod.), představují lokalizační údaje. Návrh na odpovídající rozšíření postrádá rovněž Stanovisko WP 29 k používání lokalizačních údajů se zřetelem ke službám s přidanou hodnotou z listopadu 2005.[4] Uznává však, že lokalizační údaje jsou mnohdy „velmi citlivé", a doporučuje nejpozději do dvou měsíců od jejich vytvoření provést anonymizaci.

Z nerespektování pravidel pro zpracování lokalizačních údajů vyvodil procesní důsledky například francouzský Kasační soud v rozhodnutí ze dne 6. 4. 2004, kdy neuznal výpověď danou zaměstnanci, který odmítl užívat kartu umožňující kontrolu příchodů a odchodů. Soud konstatoval, že jelikož předmětný monitorovací systém nebyl ohlášen francouzskému úřadu pro ochranu osobních údajů (dále jen „CNIL"), takto opatřené důkazy jsou procesně nepřípustné.[5]

Specifickým tématem je směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (dále jen „DRD"). Úpravy členských států implementující tuto směrnici ukládají povinným osobám (poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí) uchovávat provozní údaje a lokalizační údaje a související údaje nezbytné k identifikaci účastníka nebo uživatele. Není pochyb, že z těchto informací lze sestavit podrobný profil jednotlivce, a to do značné míry včetně predikce jeho chování.[6]

Oproti tomu, některé právní řády strukturují pojem osobní údaj do více kategorií, než předpokládá DPD. Estonský zákon vymezuje tripartici osobních údajů: osobní údaje, citlivé osobní údaje a soukromé osobní údaje.[7] Italský zákon zakotvuje speciální kategorii soudních údajů.[8] Maďarský zákon počítá se zvláštními údaji a trestněprávními osobními údaji.[9]

Směrnicová definice zahrnuje též informace se vzdálenější vazbou k podoblasti jednotlivcova soukromí pokládané za citlivou. Ve Francii je zmiňovaná nepřímá identifikace (zahrnující kupř. souvislost mezi gastronomickými zvyklostmi a náboženských vyznáním) výslovně přiřazena problematice citlivých údajů. Za zaznamenání stojí, že některé právní řády (Finsko, Irsko, Rakousko, Řecko, Spojené království a Spolková republika Německo) pojem citlivý údaj nedefinují s použitím výrazu „odhalující", nýbrž uvažují „údaje o"; tím je ovšem naznačena užší vazba k subjektu údajů, z níž by měl vyplývat závěr, že ty informace, které slouží pouze k nepřímé identifikaci charakteristik podle čl. 8 odst. 1 DPD, citlivý údaj nepředstavují.

---

[2] Data Protection Act 1998: Post-Implementation Appraisal. Dostupné z http://www.dca.gov.uk/ccpd/dparev.htm.

[3] The 2002 Proposals for Amendment of the Data Protection Directive (95/46/EC), made by Austria, Finland, Sweden and the United Kingdom – Explanatory Note. Dostupné z http://www.dca.gov.uk/ccpd/dpdamend.htm.

[4] Working Party 29 Opinion on the use of location data with a view to providing value-added services. Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

[5] 01-45.227 Arrêt n° 944 du 6 avril 2004 Cour de cassation - Chambre sociale. Dostupné z http://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/arret_no_1063.html

[6] Eagle N., Pentland, A.: "Eigenbehaviors: Identifying Structure in Routine", Behavioral Ecology and Sociobiology, 2009, 63:7, 1057-1066. Dostupné z http://reality.media.mit.edu/ pdfs/eigenbehaviors.pdf.

[7] Estonský zákon o ochraně osobních údajů (RT I 2003, 26, 158), § 4. Dostupné z http://www.legaltext.ee/en/andmebaas/tekst.asp?loc=text&dok=X70030&keel=en&pg=1&ptyyp=RT&tyyp=X&query=data%2BprotectionLink.

[8] Italský zákoník ochrany osobních údajů přijatý zákonným dekretem no. 196 ze dne 30. 6. 2003, čl. 4 odst. 1 písm. e). Dostupné z http://www.dataprotection.it/codice_privacy_ english.htm

[9] Maďarský zákon LXIII z roku 1992 o ochraně osobních údajů a přístupu veřejnosti k údajům ve veřejném zájmu, čl. 2 odst. 2 a 3. Dostupné z http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII.

„Nepřímou identifikovatelnost“ mohou v některých případech chtít omezovat samotní zaměstnavatelé, kupříkladu kvůli předpokládaným názorům zákazníků. Pohybují se na tenkém ledě kvůli riziku střetu s antidiskriminačním právem, avšak ani zde nejsou bez šance. Příkladem je rozhodnutí ve věci Kara v. Spojené království, kde Evropská komise pro lidská práva konstatovala, že soudy nepochybily aprobováním postupu zaměstnavatele, který zakázal svému zaměstnanci nosit ženské oblečení; neopomenula přitom zdůraznit, že se toto opatření týkalo jen pracovní doby.[10]

## *2. Zpracování „citlivých údajů“*

### 2.1. Obecná a speciální pravidla zpracování

Je nabíledni, že zákaz zpracování citlivých údajů nemůže být absolutní. Zákaz podle čl. 8 odst. 1 DPD se nepoužije, pokud nastane některá z podmínek předvídaných v odstavci bezprostředně následujícím. Stanovené výjimky vyčleňují předmětné citlivé údaje z režimu čl. 8 odst. 1 DPD, ale nikoli z dosahu obecných pravidel dopadajících na zpracování osobních údajů.

I pokud je splněna některá z podmínek dle druhého odstavce čl. 8 DPD, dopadají na zpracování citlivých údajů další regulační mechanismy. V této souvislosti představuje základní nástroj předběžná kontrola vycházející z čl. 20 DPD, byť ani ta se neuplatňuje bez výjimek.

Kupříkladu podle německého spolkového zákona není předběžná kontrola požadována, pokud: je dán zákonný závazek provést zpracování, subjekt údajů udělil souhlas, nebo zpracování je v souladu se smlouvou uzavřenou se subjektem údajů. Vzhledem k této dodatečné zátěži se doporučuje správcům osobních údajů náležitě uvážit, zda je zpracování citlivých údajů vskutku nutné. Uvedený zákon výslovně stanoví, že tyto údaje musejí být vymazány, pokud správce údajů nemůže prokázat, že jsou přesné.[11]

### 2.2. „Výslovný souhlas“

Podle výjimky zakotvené v čl. 8 odst. 2 písm. a) DPD je zpracování citlivých údajů přípustné, pokud k němu subjekt údajů udělí výslovný souhlas, ledaže právní předpisy členského státu stanoví, že zákaz uvedený v odstavci 1 nelze zrušit udělením souhlasu subjektu údajů. Takto kvalifikovaný souhlas je založen na zásadě opt-in, tj. na potvrzujícím úkonu subjektu údajů, kterým se jasně dává najevo souhlas se zpracováním. Jinak řečeno, souhlas vycházející ze zásady opt-out nebude postačující.

Písemný souhlas zaměstnance (či uchazeče o zaměstnání) není považován za legitimní podklad pro zpracování citlivých osobních údajů podle královského dekretu provádějícího belgický zákon o ochraně osobních údajů.[12] Podle německého spolkového zákona souhlas musí být udělen písemně a výslovně odkazovat na citlivé údaje, jinak je neplatný.[13] Česká právní úprava nestanoví dodatečné požadavky nad rámec DPD.[14]

Jedna z metod, jak v on-line prostředí dosáhnout právoplatného výslovného souhlasu, se nazývá Just-In-Time Click-Through Agreements (JITCTA).[15] Je založena na zjištění, že souhlas s obsáhlými obchodními podmínkami, které by – mimo jiné – zahrnuly dispozice s citlivými údaji, má jen formální povahu a z hlediska aplikace čl. 8 odst. 2 písm. a) DPD je jeho hodnota sporná. V případě uplatnění JITCTA uživatel vyslovuje s využitím dialogového okna (srov. PRIME IPV2) souhlas se zpracováním osobních údajů jen v jednotlivostech, v návaznosti na to, jaké kroky skutečně činí (a tedy, jaké citlivé údaje budou vskutku předány ke zpracování). Přijatelnou možností je vyjádření souhlasu dvojitým kliknutím; prvním potvrdíme, že jsme si vědomi požadovaného zpracování a druhým dáme výslovně najevo souhlas.

### 2.3. Kvalifikovaná „nezbytnost“ zpracování

Další právní důvody pro zpracování citlivých údajů zakotvené ve druhém odstavci čl. 8 se již neodvíjejí z výslovného souhlasu, ale zejména odkazují na pojem „nezbytnost“ ve spojení s určitým právem aprobovaným zájmem. Předmětná norma DPD užitím pojmu „nezbytný“ nedává široký prostor pro své dotváření interpretací; přítomnost jisté „diskreční pravomoci“ se

[10] Rozhodnutí EKLP ze dne 22. 10. 1998 ve věci Kara v. Spojené království, stížnost č. 36528/97.

[11] Spolkový zákon o ochraně osobních údajů, čl. 4d odst. 5, resp. § 35 odst. 2 bod 2. Dostupné z http://www.bfdi.bund.de/cae/servlet/contentblob/411288/publicationFile/25384/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf.

[12] Čl. 27 belgického královského dekretu. Dostupné z http://www.privacycommission.be/en/static/pdf/wetgeving/royaldecree -2001-september-2009.pdf.

[13] Spolkový zákon o ochraně osobních údajů, čl. 4a odst. 3. Dostupné z http://www.bfdi.bund.de/cae/servlet/contentblob/411288/publicationFile/25384/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

[14] § 9 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů.

[15] Fischer-Hübner, S., Pettersson, J. S., Bergmann, M., Hansen M., Pearson, S., Mont, M. C.: HCI Designs for Privacy-enhancing Identity Management, in: Acquisti, A., De Capitani di Vimercati, S., Gritzalis, S., Lambrinoudakis, C. (eds.): Digital Privacy: Theory, Technologies and Practices, Auerbach Publications (Taylor and Francis Group), 2007, s. 241.

v tomto směru naznačuje jen poukazem na „vnitrostátní právní předpisy".

### 2.3.1. Pracovní právo

Dle písm. b) představuje další výjimku nezbytnost zpracování pro dodržení povinností a zvláštních práv správce v oblasti pracovního práva, pokud je k tomu oprávněn vnitrostátními právními předpisy, které stanoví příslušná ochranná opatření.

Uvedený případ může nastat kupř. tehdy, pokud zákon ukládá obchodní společnosti srážet zaměstnancům ze mzdy částky k úhradě příspěvků odborové organizaci, jejímiž jsou členy, nebo vést evidenci zaměstnanců se zdravotním postižením za účelem aplikace příslušných pracovněprávních opatření. K tomu lze poukázat na zákon o ochraně osobních údajů rakouský (§ 9), belgický (čl. 6 odst. 2), irský (§ 3 písm. b/) a švédský (§ 16).

Stanovené výjimky se uplatní jen tehdy, pokud je příslušné pravidlo obsaženo v zákonné normě nebo alespoň tato norma zmocňuje k jeho vydání orgán působící v oblasti pracovních vztahů, kupř. radu zaměstnanců).

Jelikož jde, jak bylo řečeno, o restriktivně interpretovatelnou výjimku, zpravidla nebude dostatečným právním základem pro předávání údajů zaměstnance jednou právní entitou druhé, a to i tehdy, jsou-li obě součástí stejné skupiny.

Francouzský zákon výjimku týkající se dodržení povinností a zvláštních práv správce v oblasti pracovního práva neimplementoval. Nad to CNIL dne 5. 7. 2005 přijal soubor doporučení zaměstnavatelům, jak předcházet „etnicko-rasové diskriminaci" (diskriminace je postižitelná dle čl. 122-45 zákoníku práce a čl. 225 odst. 1 trestního zákona).[16] Úřad vymezil údaje, z nichž by se diskriminace mohla odvíjet (jméno a příjmení, současná i „původní" národnost, místo narození, národnost a místo narození rodičů, adresa). Etnicko-rasové indikátory se nevyskytují ve veřejných statistikách. Zaměstnavatelé by neměli evidovat původní národnost zaměstnance (uchazeče o zaměstnání) nebo národnost či místo narození jeho rodičů. Jestliže jsou vedeny statistiky (resp. vyhotovena odpovídající studie) ohledně etnického složení pracovišť, je třeba mít na paměti, že jediným účelem jejich zpracování zůstává zajišťování rasové, národnostní a etnické „diverzity" personálního zázemí organizace. Je otázkou, zda požadavek na utajení některých charakteristik zaměstnanců – vnímaných jako citlivých – se neobrátí proti osobám, které má chránit, neboť organizace může s poukazem na uvedený režim skrýt „nediverzifikovanost".

Úřad v témže dokumentu doporučil zpracování životopisů uchazečů o zaměstnání až poté, co budou identifikační údaje odděleny od věcné náplně tohoto dokumentu. V této souvislosti se doporučuje, aby přijímací řízení bylo realizováno tak, že životopisy s kontaktními údaji obdrží jiná organizační složka zaměstnavatele (nebo externí personální agentura) a ta je předá již anonymizované k posouzení jinému oddělení (resp. samotnému zaměstnavateli) k vyhodnocení. Je zřejmé, že význam tohoto opatření omezuje okolnost, že „druhé kolo" výběrového řízení zahrnující pohovor s uchazeči již podobně anonymní být nemůže.

### 2.3.2. Obrana životně důležitých zájmů

Výjimka dle písm. c) se týká zpracování nezbytného k obraně životně důležitých zájmů subjektu údajů nebo jiné osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas. Irská úprava rozšiřuje tuto výjimku i na prevenci škody na majetku, čímž se od dikce DPD odchyluje.[17]

### 2.3.3. Údaje členů společenských organizací

Výjimka dle písm. d) se týká zpracování prováděného společenskými organizacemi v rámci jejich legitimních činností a s odpovídajícími zárukami nadace, sdružení nebo jakýkoli jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíly, a že tyto údaje nejsou sdělovány třetím osobám bez souhlasu subjektu údajů. Jde o ustanovení chránící vybrané organizace před nepřiměřenou administrativní zátěží, neboť se má samo sebou, že již žádostí o členství v příslušné organizaci se dává (byť implicitní) souhlas se zpracováním údajů a snížení ochrany soukromí je vyváženo přínosem z kolektivní akce.[18]

[16] Lutte contre les discriminations: les recommandations de la CNIL pour mesurer la diversité des origines. Dostupné z http://www.cnil.fr/dossiers/travail/actualites/browse/5/article/554/lutte-contre-les-discriminations-les-recommandations-de-la-cnil-pour-mesurer-la-diversite-des-ori/

[17] Irský zákon o ochraně osobních údajů, 2B-(1), písm. b), (iii). Dostupné z http://www.dataprotection.ie/viewdoc.asp?DocID=796&ad=1.

[18] V širších souvislostech srov. Olson, M.: The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press, Cambridge, 1971.

### 2.3.4. Údaje očividně zveřejňované nebo související s právními nároky

Výjimka ve smyslu písm. e) zahrnuje zpracování údajů očividně zveřejňovaných subjektem údajů nebo nezbytných pro zjištění, uplatnění nebo obranu právních nároků před soudem.

V britském zákoně se poukazuje na učinění údajů veřejnými „coby výsledek uváženě přijatých kroků subjektu údajů“.[19] Toto je poněkud překvapivé v kontextu celkového liberálního přístupu britského zákonodárce k implementaci DPD. Ochrana údajů se totiž odvíjí z ústavně zaručeného práva na soukromí, a tedy nemůže být prostředky „jednoduchého“ práva eliminována; zároveň však i ústavněprávní normy členských států aprobují autonomii vůle, a tudíž nelze nepřiměřeně „direktivně“ vnucovat jednotlivci způsoby nakládání s vlastními údaji. Zatímco u jiných lidských práv (s výjimkou zejména jejich tzv. tvrdého jádra) přichází do úvahy omezení (v některých případech smluvní), ohledně práva na ochranu soukromí ve smyslu čl. 8 Úmluvy může – v určitých situacích – samotná smlouva (či jiný projev vůle) rozsah pojmu soukromí vymezit. Uvedené dokládá rozhodnutí Evropského soudu pro lidská práva ve věci Halford v. Spojené království uznávající „upozornění“ zaměstnavatele na odposlech coby kritérium určující legitimní očekávání uživatele telefonu.[20]

„Očividné zveřejňování“ však může být omezováno nikoli kvůli subjektům údajů, ale též pro ochranu „příjemců“ těchto informací. Toto hledisko uplatňoval předseda řecké Národní rady pro rozhlas a televizi, který – bezúspěšně – usiloval o zákaz vysílání tamější verze soutěže Big Brother.[21]

Není pochyb, že pro (neuvážlivého) jednotlivce by v některých případech bylo lépe, kdyby ani očividně zveřejněné citlivé údaje nemohly být dále zpracovány. Lze připomenout známou (byť již judikatorně ve své původní formě překonanou) sentenci soudce O. W. Holmese, podle níž policista má ústavní právo vyjadřovat se k politickým otázkám, ale ne ústavní právo být policista.[22]

[19] Schedule 3. Conditions relevant for purposes of the first principle: processing of sensitive personal data. Odst. 5. Dostupné z http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10#sch3.

[20] Rozsudek ESLP ze dne 25. 6. 1997 ve věci Halford v. Spojené království, stížnost č. 20605/92.

[21] Ban on Greek Big Brother overturned, 22. 3. 2002. Dostupné z http://news.bbc.co.uk/2/hi/entertainment/1886998.stm.

[22] McAuliffe v. Mayor of City of New Bedford, 29 N.E. 517, 517-518 (1892).

## 2.4. Zdravotní a související údaje, profesní tajemství ve zdravotnictví

Podle třetího odstavce čl. 8 DPD se odstavec 1 (tj. zákaz zpracování citlivých údajů) nepoužije, je-li zpracování údajů nezbytné pro účely zdravotní prevence, lékařských diagnóz, lékařské péče a ošetřování nebo správy zdravotnických služeb a pokud tyto údaje zpracovává odborný zdravotnický pracovník, který je na základě vnitrostátního práva nebo právních předpisů přijatých příslušnými vnitrostátními orgány vázán povinností zachovávat profesní tajemství, nebo jiná osoba rovněž podléhající obdobné povinnosti mlčenlivosti.

### 2.4.1. Genetika

S touto problematikou úzce souvisí zpracování genetických údajů. V zákonech některých členských států (včetně České republiky) jsou genetické údaje samostatnou kategorií v taxonomické řadě citlivých údajů. V Lucembursku jde o informace o dědičných vlastnostech jednotlivce nebo specifické skupiny jednotlivců.[23] V souvislosti s genetickými údaji přijala striktní stanovisko lucemburská Národní komise pro ochranu údajů, dle něhož ustanovení čl. 6 zákona o ochraně osobních údajů ze dne 2. 8. 2002 je třeba vykládat tak, že zpracování osobních údajů vycházejících z genetických informací je přípustné jen v rámci soudního řízení, tj. kupříkladu paternitního sporu.[24] Toto řešení zohledňuje fakt, že potřebný genetický materiál bude z logiky věci získán bez právoplatného souhlasu samotného dítěte (odhlédneme-li od situace, kdy jde o „prověření“ otcovství k dítěti již zletilému), a byť nekoliduje s dosavadní judikaturou Evropského soudu pro lidská práva, je patrné, že nesleduje její určitý vývoj směrem k rozšíření právních možností dosažení shody stavu „matrikového“ s „biologickým“.[25]

[23] Lucemburský zákon o ochraně osobních údajů z 2. 8. 2002, čl. 2 písm. g). Dostupné z http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf.

[24] À propos de la licéité des tests de paternité. 18. 1. 2005. Dostupné z http://www.gouvernement.lu/salle_presse/communiques/2005/01/18test_paternite/index.html.

[25] Rozsudek ESLP ze dne 24. 11. 2005 ve věci Shofman v. Rusko, stížnost č. 74826/01, a ze dne 10. 10. 2006 ve věci Paulík v. Slovensko, stížnost č. 10699/05, dále též rozsudek německého Spolkového ústavního soudu ze dne 12. 2. 2007, sp. zn. 1 BvR 421/05.

### 2.4.2. Webové stránky se zdravotnickou tématikou

Ne vždy jsou zdravotní údaje (mnohdy s nezanedbatelnou vypovídací hodnotou) v dosahu lékařského tajemství. [26] Kupříkladu dne 8. 3. 2001 CNIL vydal doporučení týkající se webových stránek věnovaných problematice zdravotní péče.[27] Toto doporučení vychází z prověření více než 60 webů a odtud vyplývajícího zjištění, že řada z nich nesplňuje zákonné požadavky na ochranu osobních údajů. Uvedené stanovisko tezí, že „údaje ohledně zdravotní péče o identifikovaném nebo identifikovatelném jednotlivci by neměly být kupovány ani prodávány, a to ani tehdy, pokud dotčená osoba s touto dispozicí udělí souhlas", přistupuje ke zdravotní péči coby k veřejnému statku, což jde nad rámec požadavků DPD. Proti komerčnímu využití citlivých údajů získaných správci webových stránek se zdravotní tématikou směřuje rovněž požadavek, aby provozní údaje vztahující se k jejich návštěvám byly pokládány za citlivé údaje, spojují-li se s dalšími údaji ohledně zdravotního stavu (například s vyplněným dotazníkem zabývajícím se zdravotními problémy), a nebyly předávány pojišťovnám, bankám nebo zaměstnavatelům. V tomto duchu se nese též doporučení, aby veřejné orgány vykonávaly náležitě kontrolní pravomoc.

### 2.4.3. Biotechnologie a biometrie

Biotechnologie jsou označovány za novou průmyslovou revoluci.[28] Ačkoli jde o téma kontroverzní, protichůdnost názorů může být jen zdánlivá, jak dokládá studie, která poukazuje, že neexistuje jednoznačná pozitivní korelace mezi religiozitou jednotlivce a záporným či pesimistickým pohledem na biotechnologie, včetně klonování a využití kmenových buněk.[29] Citovaná studie ovšem zdůrazňuje, že Američané jsou v mezinárodním srovnání k biotechnologiím vstřícnější než většina jiných národů.

Méně kontroverzní matérii než biotechnologie představují metody biometrie. Tím, že vycházejí z biologických charakteristik člověka, jsou údajům zpracovávaným pro zdravotnické účely blízké biometrické údaje. Biometrie zahrnuje autentifikaci na základě rozpoznání zejména DNA, oční sítnice nebo duhovky, otisku prstů nebo dlaně, charakteristik obličeje, geometrie kontur ruky, hlasu a rukopisu nebo dynamiky stisku kláves.[30]

Není pochyb, že biometrické údaje mohou být z hlediska ochrany soukromí mnohdy zcela neškodné, v jiných případech je tento jejich rozměr zásadní. Zde se coby nedostatek projevuje správněprávní metoda regulace osobních údajů, která bez pravidla *de minimis* neumožňuje patřičnou diferenciaci situací z hlediska rizika pro soukromí.[31]

Specifickým zařízením napomáhajícím v boji proti mezinárodnímu terorismu na letištích je tělesný scanner, který umožňuje vidět skrz oděv např. zbraně nebo plastické výbušniny.[32] Přístroj zobrazuje procházející cestující jakoby bez oblečení. Zároveň jej lze nastavit tak, že pro obsluhu „zneviditelní" obličej procházející osoby. Přestože je pravděpodobnost odhalení nebezpečných předmětů prakticky shodná, Jeffrey Rosen, autor knihy[33], které uvedené zařízení dalo název, zaznamenal, že mnozí lidé přesto dali přednost kontrole bez této úpravy. Proti zavedení podobných opatření na evropských letištích, doposud využívaných jen pro transatlantické lety z Itálie, Nizozemska a Spojeného království se ovšem zvedl odpor též ze strany poslanců Evropského parlamentu.[34] Oponenturu nevyvrátil ani argument, že pracovník pověřený sledováním výstupů tohoto scanneru nebude znát totožnost kontrolované osoby.

Vzhledem k omezení dosahu DPD daného jejím čl. 3 odst. 2 (které ovšem nepřevzaly všechny členské státy) může být problematická harmonizace této problematiky dle předpisů implementujících uvedenou směrnici. Se zřetelem k poměrně extenzívnímu výkladu čl. 95 DPD podanému Evropským soudním dvorem ve věci C-301/06 ve vztahu k DRD – týkajícího se pro-

[26] Odpověď zdravotnického zařízení českému soudu s poukazem na lékařské tajemství může znít následovně: K Vaší žádosti sdělujeme, že jsme si dne … vyžádali souhlas pacienta … s podáním zprávy soudu, odpověď jsme dosud neobdrželi. Bez tohoto souhlasu požadované informace nelze podat s ohledem na povinnost mlčenlivosti uloženou zdravotnickým pracovníkům ustanovením § 55 odst. 2 písm. d) zákona č. 20/1966 Sb., v účinném znění, jejíž porušení je trestné dle ust. §180 tr. zákoníku.

[27] Délibération No. 01-011 du 08 mars 2001 portant adoption d´une recommandation sur les sites de santé destinés au public. Dostupné z http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222335&categorieLien=cid.

[28] Scheitle, C. P.: In God We Trust: Religion and Optimism Toward Biotechnology. Social Science Quarterly, 2005, Volume 86, Number 4, 2005, s. 846.

[29] Tamtéž, s. 854.

[30] Biométrie. Dostupné z http:// www.cnil.fr/fileadmin/ documents/approfondir/dossier/CNI-biometrie/ LA_BIOMETRIEmai2005.pdf.

[31] Polčák, R.: Some Notes on Current Paradoxes in the Law on Personal Data Protection. s. 53. Dostupné z http://www.infojog.hu/sites/infojog.hu/files/polcak_some_notes.pdf.

[32] Ovšem s nikoli zanedbatelnou výjimkou těch látek, které by terorista po vzoru pašeráků drog spolkl.

[33] Jeffrey, R.: The naked crowd: reclaiming security and freedom in an anxious age, Random House, 2005.

[34] Na koho si posvítit? Na cestující anebo na teroristy? 29. 1. 2010. Dostupné z http://www.europarl.europa.eu/news/ public/story_page/031-67880-025-01-05-903-20100121STO67830-2010-25-01-2010/default_cs.htm.

blematiky v první řadě bezpečnostní – není patrně vyloučeno aplikovat implementační úpravu i na tyto kontroly.

## *3. Výjimky podle práva členského státu – odstavce čtvrtý a pátý*

### 3.1. Obecná charakteristika

Odstavce čtvrtý a pátý DPD zmocňují členské státy k legislativnímu zakotvení též dalších výjimek, a to „z důvodu významného veřejného zájmu", respektive ve vztahu k „zpracování údajů týkajících se protiprávního jednání, rozsudků v trestních věcech nebo bezpečnostních opatření" (pojem bezpečnostní opatření normativně předvídaný tímto ustanovením odkazuje na nástroje trestního práva, jakými je kupř. probace nebo domácí vězení). Některé členské státy pravomoci odvíjející se z čl. 8 odst. 4 a 5 DPD využily, což dokládá finský zákon o ochraně osobních údajů a obdobný italský předpis.[35] Další členské státy rovněž vyžadují povolení úřadu pro ochranu osobních údajů před zpracováním osobních údajů. Srov. dánský zákon o ochraně osobních údajů, který zpracování citlivých údajů vyžadujících oznámení úřadu pro ochranu osobních údajů podmiňuje předchozím povolením tohoto úřadu.[36] Odchylky z odstavce 1 stanovené v odstavcích 4 a 5 se oznamují Komisi.

### 3.2. Odstavec čtvrtý – významný veřejný zájem

Podle odstavce čtvrtého čl. 8 DPD platí, že jsou-li poskytnuta vhodná ochranná opatření, mohou členské státy určit z důvodu významného veřejného zájmu i jiné výjimky, než jaké jsou stanoveny v odstavci 2 buď prostřednictvím vnitrostátních právních předpisů, nebo rozhodnutím orgánu dozoru.

Této možnosti využila řada členských států. Zákon ve Spojeném království vymezuje s poukazem na čl. 8 odst. 4 DPD následujících 5 situací: podstatný veřejný zájem; prevence nebo odhalení nezákonného činu; ochrana veřejnosti před určitým chováním, které nepředstavuje nutně nezákonný čin, ale jde kupř. o nekompetentní výkon řídících funkcí; zveřejnění pro žurnalistické, umělecké nebo literární účely, je-li takové zveřejnění ve veřejném zájmu (upozorňuje se jím na nezákonné jednání apod.); poskytování některých služeb, pokud je to podmínkou pro jejich realizaci a subjekt údajů nemůže souhlas vyslovit. Ve Francii byla s poukazem na čl. 8 odst. 4 DPD vydána řada speciálních zákonů a dekretů týkajících se zdravotních záznamů nebo veřejné bezpečnosti.

### 3.3. Odstavec pátý – údaje z právních řízení

Podle odstavce pátého zpracování údajů týkajících se protiprávního jednání, rozsudků v trestních věcech nebo bezpečnostních opatření lze provádět pouze pod kontrolou orgánu veřejné moci nebo pokud vnitrostátní právo stanoví vhodná zvláštní ochranná opatření, s výhradou výjimek, které mohou být uděleny členským státem na základě vnitrostátních předpisů upravujících vhodná zvláštní ochranná opatření. Úplná sbírka rozsudků v trestních věcech musí být v každém případě vedena pod kontrolou orgánu veřejné moci. Členské státy mohou stanovit, že údaje týkající se správních sankcí nebo rozsudků v občanských věcech budou rovněž zpracovávány pod kontrolou orgánu veřejné moci.

Jen některé státy pokládají trestní záznamy za citlivé údaje a v určitých případech je diskutabilní, zda předmětný osobní údaj spadá mezi citlivé. Lze jmenovat právě údaje podle čl. 8 odst. 5 DPD týkající se protiprávního jednání, rozsudků v trestních věcech nebo bezpečnostních opatření. Vyvstává kupříkladu otázka, zda zadržení policií bez následného vznesení obvinění bude spadat pod dosah tohoto ustanovení.

Některé členské státy zakazují zpracování osobních údajů týkajících se trestných činů i tehdy, je-li subjektem osobních údajů poskytnut souhlas. Toto normativní řešení působí problémy zaměstnavatelům, kteří chtějí prověřit uchazeče o zaměstnání podle výpisu z rejstříku trestů, což je případ Belgie a Lucemburska, jejichž zákony mezi citlivé zařazují údaje z právních řízení.[37]

Právní řády členských států v souvislosti s předmětnými údaji zakotvují požadavek předběžné kontroly a testy proporcionality. Výjimky dopadají na zpracování údajů obhájci a dalšími právními zástupci, pakliže se výkon těchto profesí v dosahu zákonů o ochraně osobních údajů nachází.

Byť Úmluva o ochraně lidských práv a základních svobod nevymezuje samostatně kategorii citlivých údajů, z anonymizace právě těch rozhodnutí Evropského soudu pro lidská práva (resp. orgánů Úmluvy), která se týkají obdobných otázek, na něž pamatuje výše uvedenou speciální úpravou evropské směrnicové právo, je zřejmé, že k tomuto rozlišení přihlíží.

[35] § 12 odst. 1 bod 4 finského zákona. Dostupné z http://www.tietosuoja.fi/uploads/hopxtvf.HTM. Čl. 24 odst. 1 písm. f) italského zákona. Dostupné z http:// www.dataprotection.it/codice_privacy_english.htm.

[36] Srov. § 50 odst. 1 dánského zákona. Dostupné z http:// www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/.

[37] Čl. 8 belgického zákona a čl. 8 odst. 2 lucemburského zákona, viz výše.

Specifickou kategorií quasi-citlivých údajů jsou v některých členských státech uznány informace z trestních či obdobných řízení ve věcech mládeže. Je tomu tak proto, že publicita projednávané věci by odsouzeného trvale stigmatizovala a ztížila resocializaci, která je u mladistvých pachatelů pravděpodobnější. K uvedenému lze poukázat na čl. 40 Úmluvy o právech dítěte. V České republice platí zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), který zvýšenou ochranu osobních údajů zakotvuje ve svém § 3 odst. 5 zákona a dále v ustanoveních §§ 52–54. Ustanovení § 54 předepisuje, že rozsudek se vyhlašuje veřejně, současně ale stanoví omezení jeho medializace.

## 4. Národní identifikační číslo

Členské státy určí podmínky, za kterých může být předmětem zpracování vnitrostátní identifikační číslo nebo jakýkoli jiný identifikátor obecného významu. Za zmínku stojí, že některé státy umožňují jeho používání v soukromém sektoru na podkladě souhlasu, případně doplněného „jasným ospravedlněním" jako je tomu ve Švédsku, jinde se uplatňují omezení též z obavy z důsledků vzájemného propojení databází, v důsledku čehož zpracování vyžaduje souhlas úřadu pro ochranu osobních údajů.[38]

## Závěr

Citlivé údaje jsou směrnicí vymezeny nikoli v úplnosti, protože nezahrnují ekonomické a lokalizační údaje a nedoceňují problematiku vytváření profilů jednotlivce na základě „běžných" osobních údajů. Upřesnění by si též zasloužilo určení údajů nepřímo identifikujících „citlivé" charakteristiky. Naznačené rozšíření by však učinilo definici citlivých údajů prakticky bezbřehou, což by znamenalo přinejmenším dodatečné administrativní náklady. Lze přisvědčit názoru, že pravidla obsažená v DPD (a ji implementujících zákonech členských států) by měla být aplikovatelná právě tehdy, je-li ve hře reálná hrozba pro ochranu soukromí. To platí tím spíše pro zvláštní kategorii citlivých údajů. Současně můžeme předpokládat, že naznačená změna DPD by zvýšila nároky na správce údajů, ale též úřady pro ochranu osobních údajů, neboť posouzení proměnlivých souvislostí, z něhož se míra „citlivosti" údajů odvíjí, nepředstavuje snadný úkol.


## Summary

Informations in enhanced regime of the protection by the EU Law: sensitive data. The text discusses the special privacy protection defined in the article 8 of the Data Protection Directive (Directive 95/46/EC). *The basic norm says* that member states of the European Union shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Exceptions which permit this processing are following:

- the explicit consent of the data subject, which can be problematic in the online environment,
- data is manifestly made public by its subject,
- data is concerned with the membership in specified organizations or
- the necessity associated with a particular interest which is recognized by the law, these values relate to the employment law matters, the vital interests, the defence of legal claims and the health-care services.

Restrictions also impact on the processing of data relating to law proceedings. One of the weaknesses of the Data Protection Directive is the silence about economic and location data. The issue of the indirect identification by non-sensitive characteristics is not explicitly solved in the directive. It can be a source of controversy that the concept of sensitive data is criticisable for its too close relations with anti-discrimination law.


[38] Čl. 22 švédského zákona. Dostupné z http://www.sweden.gov.se/content1/c6/01/55/42/b451922d.pdf.