Zásady ochrany osobních údajů v právu Evropské unie

Daniel Novák*

1. Prameny zásad ochrany osobních údajů

Právní zásady se vyznačují jednak vyšší obecností než právní pravidla, jednak určitým stupněm závažnosti.[1] Obecností mohou právní zásady přesahovat specifické oblasti právní regulace a dopadat na právní řád jako celek. Ve středu pozornosti příspěvku však jsou zásady vlastní podstatně úžeji vymezené problematice ochrany osobních údajů. Druhou součástí definice právního principu je poukaz na společenský význam: právní zásada musí vyjadřovat některou z ústředních hodnot právní materie stojící v jejím dosahu.

Praktický význam právního principu je dán též jeho způsobilostí zajistit překlenutí mezer v právních pravidlech, což nabývá zvláštního významu v případě ochrany osobních údajů, kde se vzhledem k proměnlivosti vztahů, které jsou předmětem úpravy, technologickým vývojem často nelze argumentaci právními zásadami vyhnout. V této souvislosti stojí za zaznamenání, že nesprávný výklad by v prostředí Evropské unie, kde ochrana lidských práv spadá mezi obecné zásady jejího práva a čl. 6 odst. 1 Smlouvy o Evropské unii ve znění Lisabonské smlouvy přiznává Listině základních práv (včetně čl. 7 a čl. 8) právní sílu zakládacích smluv, mohl nabýt rozměru porušení primárního práva.

Základními prameny sekundárního práva EU v oblasti ochrany osobních údajů jsou směrnice Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (dále jen „DPD“) a č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „DPEC“).

Obě směrnice vycházejí z Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních údajů (dále jen „Úmluvy č. 108“) přijaté na bázi Rady Evropy a otevřené k podpisu 28. 1. 1981 ve Štrasburku, která se stala prvním (od roku 1985 platným) mezinárodně závazným právním dokumentem dopadajícím specificky na problematiku ochrany osobních údajů. V roce 2001 k ní byl přijat Dodatkový protokol o orgánech dozoru a toku údajů přes hranice. Rolv Ryssdal, bývalý předseda Evropského soudu pro lidská práva, se vyslovil, že by tento soud neměl ignorovat základní principy Úmluvy č. 108, neboť představují sektorovou implementaci čl. 8 Úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluvy“) v kontextu automatizovaného zpracovávání osobních údajů; měly by pomoci s výkladem těchto povinností.[2]

Úmluvě č. 108 předcházela Pravidla pro ochranu soukromí a přeshraničních toků osobních údajů vydaná OECD 17. 9. 1980 (dále jen „Pravidla OECD“), která se vyznačují povahou doporučení. Bez vlivu na legislativní činnost nezůstává dokument OSN Směrnice pro počítačové soubory s osobními údaji z roku 1990 (dále

* Mgr. et Mgr. Daniel Novák, doktorand na Katedře mezinárodního a evropského práva PrF MU, asistent soudce Ústavního soudu ČR, Brno.

[1] Tridimas, T. The General Principles of EU Law. Second Edition. Oxford University Press, Oxford, 2006, str. 1.

[2] Ryssdal, R. Data Protection and the European Convention on Human Rights, in Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2–4 October 1991 in Strasbourg, Strasbourg: CoE, 1992, str. 42.

jen „Zásady OSN“).[3] Z mimoevropských pramenů výrazně ovlivněných evropskými směrnicemi stojí za pozornost v listopadu 2004 na setkání ministrů APEC v Santiago de Chile schválený „Privacy Framework“.[4]

2. Zásada férového a zákonného zpracování

V Úmluvě č. 108 je předmětná zásada inkorporována do čl. 5 písm. a). DPD tento princip zakotvuje ve svém čl. 6 odst. 1 písm. a). Obdobný obsah bývá přikládán § 7 Pravidel OECD, který obrací pozornost specificky ke shromažďování údajů. V systému zásad jí náleží první místo, neboť představuje nejobecnější východisko. Zatímco požadavek na zákonnost zpracování je samozřejmý a postrádá výraznější interpretační význam, pojem férového zpracování jde nad rámec připomenutí závaznosti právních norem. Imperativ „férovosti“ se vyznačuje úzkým vztahem k transparentnosti předvídané recitálem 38 DPD, neboť včasné rozpoznání možnosti odepřít zpracování údajů je prvotním prostředkem proti zneužití pozice správcem údajů. Omezení vyplývající z principu férovosti se tedy uplatní již při získávání souhlasu podle čl. 7 písm. a) DPD.

Významem institutu souhlasu se právo ochrany osobních údajů vyčleňuje ze subdisciplín správního práva, kde se uplatňuje vertikální metoda právní regulace, a též požadavky na souhlas přibližují tento soubor norem civilistickému terénu. Pracovní skupina zřízená podle čl. 29 DPD (dále jen „WP 29“) konstatovala, že platnost souhlasu předpokládá splnění čtyř kritérií; souhlas musí být: 1. jasným a jednoznačným výrazem vůle, 2. dán svobodně, 3. specifický a 4. informovaný.[5]

Na jedné straně interaktivita moderních elektronických sítí umožňuje snazší získání souhlasu a zbavuje tak nutnosti hledat právní podklad zpracování údajů kupř. ve vyvažování zájmů podle čl. 7 písm. f) DPD.[6] Na straně druhé, správce údajů (oferent) může jen stěží bez předchozího ověření totožnosti subjektu údajů předejít neplatnosti souhlasu podle čl. 2 písm. h) DPD, kupř. kvůli nezletilosti nebo použití nesrozumitelného jazyka. Správce údajů je však povinen dbát, aby obchodní podmínky, s nimiž se souhlas pojí, nebyly příliš dlouhé, nepřehledné nebo přístupné až prostřednictvím několika hyperlinků, v důsledku čehož by zde nebyla efektivní možnost těmto podmínkám porozumět a posoudit je před udělením souhlasu.[7]

Pochybnosti, zda je subjektu údajů poskytnuta férová možnost odepřít zpracování údajů, se mohou objevit v případě dovozování souhlasu na principu opt-out. Aplikační praxe přisvědčuje výkladu, že pokud předmětné ustanovení (a contrario kupř. čl. 8 odst. 2 DPD) neobsahuje pojem „výslovný“, uplatnění principu opt-in se nevyžaduje. Podmínka obsažená v čl. 2 písm. h) DPD, tj. aby subjekt údajů projevil svůj souhlas, znamená, že z pouhé nečinnosti souhlas dovozovat nelze, a tedy existence souhlasu předpokládá určité jednání, kupř. předchozí „podmíněný“ souhlas. DPD rovněž uznává právo zakázat použití osobních údajů k určitým účelům, kupř. čl. 14 písm. b) k direct marketingu. Příkladem vyslovení neplatnosti souhlasu je rozsudek Zemského soudu v Mnichově, podle kterého neobstojí ujednání o rabatech a diskontech pro svoji netransparentnost, přičemž souhlas musí v zásadě vycházet z principu opt-in.[8]

WP 29 DPD se v souvislosti s monitorováním elektronické pošty zaměstnavatelem vyslovila, že „souhlas zaměstnanců musí být udělen svobodně, při plné informovanosti a zaměstnavatelé se nemohou spoléhat na souhlas jako na obecný prostředek legitimizace tohoto zpracování“.[9] Belgie vylučuje zpracování citlivých údajů zaměstnanců zaměstnavatelem na podkladě souhlasu, neboť vzhledem k závislému postavení nejde o souhlas získaný férově.

Některé právní řády se snaží eliminovat právní nejistotu co do platnosti souhlasu opatřeními jdoucími nad rámec DPD; jedná se o případ Itálie a Spolkové republiky Německo s obecným požadavkem na písemnou formu souhlasu, který navíc v posléze jmenovaném případě musí být pro sekundární zpracování zřetelně odlišitelný od původně uděleného. Uvedené omezení se neuplatní v oblasti elektronických komunikací, k tomu srov. německý zákon o ochraně osobních údajů v souvislosti s telekomunikačními službami.

[3] Guidelines Concerning Computerized Personal Data Files, On line http://www.unhchr.ch/html/menu3/b/71.htm.

[4] APEC Privacy Framework, dostupné z http://www.apec.org/apec/news_media/fact_sheets/apec_privacy_framework.html.

[5] Article 29 Working Party. Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. (2093/05/EN WP 114, 25. listopad 2005) str. 10–12. On line text http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

[6] Poullet, Y., Dinant, J. M. The internet and private life in Europe: Risks and aspirations. In Kenyon, A. T., Richardson, M. New Dimensions in Privacy Law. International and Comparative Perspectives. Cambridge University Press, Cambridge, 2006, str. 71.

[7] Kuner, C. European Data Protection Law. Corporate Compliance and Regulation. Second Edition. Oxford University Press, Oxford, 2007, str. 68.

[8] Rozsudek Zemského soudu v Mnichově ze dne 9. 3. 2006, žaloba č. 12 O 12679/05, on line http://medien-internet-und-recht.de/volltext.php?mir_dok_id=251.

[9] Srov. Article 29 Working Party: Working document on the surveillance of electronic communications in the workplace (5401/01/EN/Final WP 55, 29. květen 2002) str. 21. On line http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf.

3. Zásada minimality

Z této zásady vyjádřené v čl. 6 odst. 1 písm. c) a e) a potažmo v čl. 7 a 8 DPD se odvíjejí kvantitativní omezení zpracovávaných údajů na ty, které jsou nezbytné pro dosažení účelů sledovaných zpracováním, a to jednak kontrolou jejich potřebnosti a přiměřenosti, jednak v rovině časové. K uvedenému též lze poukázat na čl. 5 písm. c) Úmluvy č. 108 a navazující princip proporcionality, připomenutý kupř. v ustanovení č. 4 odst. 7 Doporučení č. R (97) 18 Výboru ministrů členským státům o ochraně osobních údajů shromažďovaných a zpracovávaných pro statistické účely (schváleno dne 30. 9. 1997). Specifický obsah náleží zásadě minimality v ustanoveních čl. 7 písm. b) až f) DPD spojujících základní podmínky zpracování údajů bez souhlasu subjektů údajů s kategorií nezbytnosti vůči zde předepsaným účelům. „Nezbytnost" představuje striktní pojem, v důsledku čehož nabývá na významu předcházení přijímaní – poukazem na ni odůvodněných – nadměrných opatření správným určením hranice, kdy ještě půjde o osobní údaj podle čl. 2 písm. a) DPD.

Z hlediska dodržování principu minimality je problematické, že zákony v Rakousku a Itálii rozšiřují – bez přímé opory v DPD, zejm. v jejím čl. 2 písm. a) – koncept ochrany osobních údajů (jejich „osobní dosah") tak, že dopadá i na právnické osoby; obdobně činí z nečlenských států Lichtenštejnsko a Švýcarsko.

Další interpretační otázkou je, zda tentýž údaj může být pro toho, kdo je způsobilý dovodit vazbu mezi údajem a konkrétní osobou, osobním – a pro ostatní nikoli. Ku podpoře kladného stanoviska (ve prospěch relativní povahy osobních údajů) lze uvést, že není-li správci údajů znám jejich konkrétní subjekt, tak jako tak nemůže splnit některé povinnosti týkající se zpracování osobních údajů, kupř. informační. K témuž závěru směřuje v 15. recitálu DPD poukaz na možnost snadného přístupu k dotčeným osobním údajům; tam, kde není k dispozici znalost vazby mezi údajem a konkrétní osobou, nemůže být o „snadném přístupu" řeč. Ve většině právních řádů členských států se vychází právě z tohoto pragmatického pojetí, byť se zřetelem nejen k technickým hlediskům identifikovatelnosti, ale též v kontextu významu těchto údajů.[10] Problematické však zůstává, že úřady pro ochranu osobních údajů mají jen omezené možnosti posoudit, zda je některý údaj citlivý, protože informace hodná zvýšené ochrany se může vytvořit až kombinací několika údajů, které samostatně stojící se jeví banální, a nikdo jiný než správce nemusí vědět, které údaje propojit.

Z hlediska principu minimality je též podstatné, kdy mezi osobní údaje řadit informace, které se s konkrétní osobou spojují jen zprostředkovaně, neboť vypovídají o předmětu, který takový vztah má. Lze předeslat, že aplikační praxe vykládá pojem identifikovatelnosti extenzívně, a to s poukazem na recitál 26 DPD, dle kterého je třeba přihlédnout ke všem prostředkům, které mohou být „rozumně použity jak správcem tak jakoukoli jinou osobou pro identifikaci dané osoby …". Pakliže je IP adresa dynamická, vytváří se při každém připojení k internetu, v ostatních případech je přiřazena pro všechna připojení ta samá. Nabízí se řešení, že o osobní údaj půjde jen ve druhém případě. Z praktického hlediska provozovatele webových stránek ale naznačené rozčlenění přínos neznamená, neboť bez dalších informací nepozná, o jakou IP adresu se jedná. Evropský soudní dvůr v rozsudku ze dne 29. 1. 2008 ve věci Promusicae (C 275/06, Sb. rozh.. s. I 271) nepřímo podpořil zhrnutí i dynamické IP adresy, je-li spojena s časovými údaji o připojení. Základní vodítko pro úpravu souborů cookie představuje čl. 5 odst. 3 DPEC, avšak kvůli jejich různorodosti je třeba doplňujících stanovisek úřadů členských států. Diskusi může vyvolávat, zda se jedná o osobní údaje v případě informací přenášených prostřednictvím radiofrekvenční identifikace (RFID), kupříkladu po prodeji zboží, na němž jsou umístěny. Že tento potenciál šířit osobní údaje mají, dokládá již směrnice italského úřadu pro ochranu osobních údajů z 9. 3. 2005, která nezbytnost „minimalizace" zdůrazňuje zvláště u chipů podkožně implantovaných.[11] Dne 28. 6. 2006, Evropská komise zveřejnila komuniké, které naznačilo úvahy o doplnění DPEC tak, aby upravovala problematiku RFID.[12] Speciální úpravu anonymizace představuje čl. 8 odst. 1 DPEC.

„Minimalizovat" je třeba nejen ty údaje, které se týkají přímo osobního života, ale taktéž oblasti hospodářské, profesní atd., včetně kupříkladu údajů o pracovní způsobilosti subjektu údajů. Ku podpoře tohoto extenzívního přístupu Evropská komise poukazuje na čl. 8 Úmluvy s vědomím, že Evropský soud pro lidská práva opakovaně odmítl argumentaci smluvního státu, podle něhož se jednání odehrávalo mimo rámec „soukromého života", a tudíž se nacházelo mimo dosah čl. 8

[10] Jinými slovy, čím „citlivější" je údaj, tím obtížnější musí být identifikace, aby na něj nedopadala úprava implementující DPD. Výjimkou z „relativistického" řešení je Švédsko, které chrání osobní údaje bez ohledu na identifikovatelnost jejich subjektu správcem/zpracovatelem, což ale znamená problémy kupř. v souvislosti s genetickými výzkumy. Srov. švédský zákon o ochraně osobních údajů. On line text http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.

[11] "Smart (RFID) Tags": Safeguards Applying to Their Use – 9. březen 2005. On line http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107.

[12] European Commission, Commission Staff Working Document, 'Communication from the Commission on the Review of the EU Regulatory Framework for electronic communications network and services', COM(2006)334 final (28 June 2006), str. 28. On line http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0334en01.pdf.

Úmluvy.[13] Za zaznamenání však stojí, že předmětné závěry bývají judikovány v souvislosti s činností bezpečnostních složek (srov. Niemietz v. Spolková republika Německo, Amann v. Švýcarsko a Rotaru v. Rumunsko) a této oblasti se směrnice dotýkají jen okrajově (čl. 3 odst. 2 DPD). Rozsudek britského Odvolacího soudu ve věci Durant v. Financial Services Authority předpokládá, že osobní údaj musí být „biografický ve význačném smyslu" (mít potřebný osobní rozměr) a dostatečně „zaměřený" na subjekt údajů[14], je však obtížně udržitelný ve světle judikatury Evropského soudního dvora, dle níž zásah do soukromého života není podmíněn tím, zda informace má povahu citlivého údaje nebo jejím zveřejněním byla způsobena újma.[15]

Prostředkem respektování zásady minimality je anonymizace. Německý spolkový zákon o ochraně osobních údajů požaduje její co nejširší uplatnění a zásadě minimality přiznává přímou vymahatelnost (srov. § 3a zákona). Specifikem rakouského práva (§ 4 odst. 1 zákona o ochraně osobních údajů) je koncept nepřímo osobních údajů, kdy identifikaci osoby brání právní překážka. Tento institut je uplatnitelný kupř. v souvislosti s transferem údajů do třetích států (tj. mimo EU), kdy se nevyžaduje souhlas rakouského úřadu pro ochranu osobních údajů (§ 12 odst. 3 zákona).[16] K respektování minimality směřuje i zpracování jen těch citlivých údajů, které jsou očividně zveřejňovány samotným subjektem údajů podle čl. 8 odst. 2 písm. e) DPD, ustanovení je však třeba coby výjimku vykládat restriktivně.

4. Zásada omezení účelem

Zásada sestává ze dvou složek. Zaprvé, osobní údaje musejí být shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Zadruhé, osobní údaje nesmějí být zpracovávány pro (sekundární) účely neslučitelné s primárním účelem, přičemž slučitelnost se vykládá úzce coby „přímá souvislost" s původním účelem. Zásadu deklaruje čl. 6 odst. 1 písm. b) DPD. V Úmluvě č. 108 ji najdeme v čl. 5 písm. b), kde se hovoří o legitimních účelech. Jde rovněž o shrnutí třetí a čtvrté zásady Pravidel OECD (§ 9 a 10). Specifikace účelu též představuje třetí princip Zásad OSN.

WP 29 shledala nelegitimním postup provozovatele webových stránek, který zveřejňoval e-mailové adresy účastníků zde probíhající diskuse[17] a konstatovala, že tzv. spyware je z logiky věci instalován utajeně, v důsledku čehož jde o „neviditelné" a „nelegitimní" zpracování[18].

Zpracování pro historické, statistické nebo vědecké účely předpokládá namísto mnohdy nedosažitelného souhlasu poskytnutí vhodných ochranných opatření, jak stanoví čl. 6 odst. 1 písm. b), čl. 8 odst. 4 DPD nebo čl. 5 písm. e) Úmluvy č. 108. Pravidla týkající se sekundárního zpracování osobních údajů pro účely výzkumu v členských státech oscilují mezi etatističtějšími řešeními se zvláštní autorizací úřadem pro ochranu osobních údajů, požadavkem na prokázání významného veřejného zájmu a podrobnou úpravou testu proporcionality na straně jedné a decentralizovanou variantou s dohledem akademického etického výboru a založením výzkumu na příslušném výzkumném plánu na straně druhé.

5. Zásada omezeného zpřístupnění údajů

Zásada v praxi znamená, že osobní údaje nesmějí být zpřístupněny s výjimkou situací, kdy je dán souhlas subjektu údajů nebo jiný zákonný důvod. Zásada je vyjádřena v čl. 5 písm. a) a b) a čl. 6 Úmluvy č. 108 a čl. 6 odst. 1 písm. a) a b), čl. 7 a čl. 8 DPD, resp. § 10 Pravidel OECD. V rozhodných souvislostech stojí za zaznamenání, že rakouský zákon o ochraně osobních údajů užívá rozdílných pojmů pro zpřístupnění údajů třetí straně a zpracovateli údajů, resp. že italský zákon terminologicky rozlišuje mezi zpřístupněním třetí osobě, která identifikovaná je a která není.

[13] European Commission, First report, Analysis and impact study on the implementation of Directive 95/46/EC in Member States 43. On line http://www.statewatch.org/news/2006/oct/com-implentation-1995-dir-techn.pdf.

[14] UK Information Commissioner, 'The Durant Case and its impact on the interpretation of the Data Protection Act 1998', 27 February 2006, 2. On line http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf.

[15] Rozsudek ESD ve spojených věcech C-465/00 a C-138/01, odst. 75.

[16] Rakouský spolkový zákon o ochraně osobních údajů. On line http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ ERV_1999_1_165.pdf.

[17] Article 29 Working Party. Privacy on the Internet: A Comprehensive EU Approach to Online Data Protection. (5063/00/EN/FINAL, WP 37, 21. listopad 2000), str. 39, On line http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

[18] Article 29 Working Party. Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (5035/01/EN/Final, WP 56), str. 12, On line http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf.

6. Zásada kvality údajů

Zásada kvality údajů znamená, že osobní údaje musejí být platné a přesné ve vztahu k tomu, co mají popsat, respektive relevantní a úplné se zřetelem k účelům, pro které mají být zpracovány. Zásada je vyjádřena v čl. 6 odst. 1 písm. d) DPD tak, že osobní údaje musejí být přesné a, je-li to nezbytné, i aktualizované. První částí tohoto principu je platnost údajů, které odpovídá rovněž požadavek zakotvený v čl. 5 písm. d) Úmluvy č. 108 DPD. K témuž směřuje druhý princip Pravidel OECD (§ 8), který odkazuje na úplnost, přesnost a aktuálnost. Existují rozdíly ohledně striktnosti, s jakou je vyžadována kontrola platnosti osobních údajů. Podle čl. 6 odst. 1 písm. d) DPD musí být přijata veškerá rozumná opatření. Zásady OSN zdůrazňují pravidelné kontroly (princip 2). Další nástroje jako Pravidla OECD nebo Úmluva č. 108 se otázce kontroly kvality přímo nevěnují, byť předpoklad zachování jistých kvalitativních parametrů se podává již ze samotné existence kontrolních mechanismů. Právní praxe musí vzít na vědomí, že v některých případech subjekt údajů sděluje údaje nesprávné záměrně a není ani v možnostech správce je ověřovat. Uvedená okolnost bývá uváděna ku podpoře závěru, že advokáti nejsou správci osobních údajů.[19]

7. Zásada bezpečnosti

Ze zásady informační bezpečnosti vyplývá, že správci údajů musí přijmout vhodná technická, organizační a personální opatření k zajištění toho, že osobní údaje nebudou nahodile nebo nedovoleně zničeny, ztraceny či upraveny nebo neoprávněně sděleny či zpřístupněny, změněny, zničeny nebo zveřejněny. Zásada je vyjádřena v čl. 7 Úmluvy č. 108 a čl. 17 DPD, resp. představuje pátý princip Pravidel OECD (§ 11).

Že je bezpečnost principem, ke kterému se lze nanejvýš přibližovat, připouští Doporučení 1/99 o neviditelném a automatickém zpracování osobních údajů na internetu prováděném softwarem a hardwarem, ve kterém se uvádí, že „v současnosti je téměř nemožné užívat internet a nebýt konfrontován s rysy vpádu do soukromí, které provázejí všechny procesy zpracování osobních údajů, přičemž jsou neviditelné subjektu údajů“.[20]

S uplatněním této zásady se počítá v nejrůznějších situacích. K tomu srov. § 41 odst. 4 dánského zákona o ochraně osobních údajů, kde se konstatuje, že osobní údaje, které jsou zpracovávány pro veřejnou správu a u nichž existuje zvláštní zájem cizích mocností na znalosti jejich obsahu, musejí být v případě války nebo za podobných okolností zničeny.

8. Zásada přístupu subjektu údajů k informacím a právo na opravu osobních údajů

Tento princip směřuje k zajištění účasti a kontroly subjektu údajů nad zpracováním údajů. „Zásada práva na přístup“ je vyjádřena v čl. 8 písm. a) a b) Úmluvy č. 108, čl. 7 písm. a), čl. 8 odst. 2 písm. a) a čl. 10–12 DPD a coby zásada otevřenosti a práva na participaci představuje šestý, respektive sedmý princip Pravidel OECD (§ 12 a 13). Prostor domáhat se opravy a výmazu je vytvořen v článcích 5 písm. d) a 8 písm. c) Úmluvy č. 108 a článku 14 písm. b) DPD. Zásada směruje k průhlednosti a otevřenosti zpracování. Každé osobě musí náležet možnost získávat v přiměřených intervalech, bez přílišných průtahů nebo nákladů a ve srozumitelné formě potvrzení o tom, zda jsou v automatizovaných souborech dat uloženy osobní údaje, které se jí týkají. Specificky se tento princip uplatní v čl. 15 DPD zakazujícím rozhodnutí, které se významným způsobem dotýká subjektu, učiněné jen na základě automatizovaného zpracování údajů. V praxi je technicky nejsložitější prosazování tohoto principu v souvislosti s přeshraničním přenosem údajů a u mezinárodně sdílených databází.

9. Zásada odpovědnosti

Zásada je vyjádřena v čl. 23 DPD, který počítá s odpovědností správce za škodu způsobenou činností neslučitelnou s vnitrostátními předpisy transponujícími tuto směrnici. Zároveň mu poskytuje možnost se částečně nebo zcela zbaven této odpovědnosti, pokud prokáže, že za vznik škody neodpovídá. Ku shodnému výsledku směřuje i ustanovení čl. 10 Úmluvy č. 108 a osmá zásada Pravidel OECD (§ 14). S tímto principem rovněž úzce souvisí zásada nezávislého dozoru, která je normativně zakotvena kupříkladu v čl. 1 Dodatkového protokolu k Úmluvě č. 108. Tento protokol neukládá konkrétní rozsah působnosti dozorového orgánu a ani nestanoví rozdělení pravomoci mezi správní dozorový orgán a soudy, spolu s DPD však vyžaduje

[19] Smejkal, V. Má pravdu Mates nebo Sokol? K ochraně osobních údajů v advokacii potřetí. Bulletin advokacie, roč. 2001, č. 3, str. 33 a násl.

[20] Working Party on the Protection of Individuals with regard to the Processing of Personal data – Recommendation 1/99 – on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware (5093/98/EN/final WP 17, 23. únor 1999). On line text http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17en.pdf.

nezávislou činnost dozorových orgánů. Byť implementací DPD došlo k zásadnímu zúžení pravomoci civilních soudů rozhodovat ve sporech týkajících se ochrany osobních údajů, je třeba vzít v potaz, že diortotickou spravedlnost (předvídanou čl. 23 DPD) nemohou efektivně zajistit správněprávní sankce, a proto musí být v potřebném rozsahu jejich pravomoc zachována (srov. § 13 českého obč. zák.). Radim Polčák se v souvislosti s DPD vyslovil tak, že ačkoli pravidla pro zpracování osobních údajů jsou poměrně striktní, v praxi mnohdy (vědomě) nebývají vynucována.[21] Lze přisvědčit, že ochrana osobních údajů bývá proto někdy pokládána za jakési soft law, přičemž důvody pro tento přístup úřadů pro ochranu osobních údajů se spatřují v relativně nedlouhé existenci tohoto souboru právních institutů, v důsledku které je namístě spíše „edukativní" než represivní činnost těchto úřadů.

10. Závěr

Zásady ochrany osobních údajů v současném vyjádření představují adekvátní základ pro dodržování práva na ochranu soukromí a osobních údajů. Podobně jako se v dlouhodobém horizontu obsahový význam slov proměňuje a přizpůsobuje době, mění se i výsledky výkladu právních zásad. Byť se objevují propracované návrhy doplnění současného katalogu zásad [22], případné zvýšení efektivity ochrany osobních údajů by mělo být situováno především do územně širší harmonizace ochrany tak, aby byla co nejvíce usnadněna mezinárodní obchodní výměna; jedná se o úkol na bázi WTO. Se zřetelem k neustálému růstu možností zpracování osobních údajů danému rozvojem informačních technologií by se měla zásada férovosti projevit s tím korespondujícím zvyšováním transparentnosti zpracování, a to v první řadě u veřejných orgánů. Standardy ochrany osobních údajů by významněji neohrozila protisměrně (ve prospěch jejich určitého omezení) účinkující – potřebná – změna čl. 9 DPD, který se nyní týká zpracování osobních údajů prováděného výlučně pro účely žurnalistiky nebo uměleckého či literárního projevu, tak, aby zahrnoval svobodu projevu bez partikulárního rozlišení.

[21] Polčák, R. Some Notes on Current Paradoxes in the Law on Personal Data Protection. Conference Essays, str. 54 http://www.infojog.hu/sites/infojog.hu/files/polcak_some_notes.pdf.

[22] Poullet, Y., Dinant, J. M. The internet and private life in Europe: Risks and aspirations. In Kenyon, A. T., Richardson, M. New Dimensions in Privacy Law. International and Comparative Perspectives. Cambridge University Press, Cambridge, 2006, str. 78 a násl.

Summary

The article discusses the privacy protection principles in the EU law. These principles are characterized by their greater generality and social importance. The protection of privacy has its human-rights dimension. In the EU law the principles are defined by the Data Protection Directive. This document draws on other sources: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and UN Guidelines Concerning Computerized Personal Data Files. Other legal acts are inspired by the DPD. The principle of fair and lawful processing lays down some requirements for valid consent of data subjects. Impacts of the principle of minimality are strengthened by the recent ECJ case law which recognizes the relatively broad scope of the concept of personal data. The purpose specification principle means that the purpose of processing personal data has to be legitimate and its changes are subject to special requirements. The disclosure limitation principle describes the fundamental defensive function of the set of norms for personal data protection. The data quality principle means that processed data should correspond with reality. But this is conditional on the willingness of data subjects. The security principle is fully respected only in theory. If a data controller has good will, implementation of the principle of data subject participation and control is facilitated by new information technologies. The accountability principle is characterized by the difference between the broadly defined competences of data protection authorities and the application practices which cause that these rules are considered "soft law". Finally, it is noted that the principles mentioned should be proportionally applied in the global context and this could be a task for the WTO.