

Přístup subjektu údajů k informacím a právo na opravu osobních údajů v evropském právu

Mgr. et Mgr. Daniel Novák

Masarykova univerzita, Právnická fakulta, Katedra mezinárodního a evropského práva, Česká republika

Abstrakt:

Access and rectification rights in the European Law

The paper analyses the personal data protection in the context of the European Law. Chapter I discusses the term of the privacy and the evolution of its meaning. Beside determining social aspects, the main tendencies of the evolution of juridical doctrines are investigated. Chapter II treats the position of the personal data protection with an emphasis on the sources of human rights in the context of the European legal culture. Chapter III contains an analysis of aspects of the access and rectification rights in European documents focused on the right to privacy and personal data protection. Chapter IV is interested in case-law of the European Court of Human Rights and the European Commission of Human Rights focusing on the access and rectification rights. The fifth chapter is an analysis of the general regime of the access and rectification rights on the background of comparison of the normative framework and the case-law of the courts of the EU Member States. In the end, I summarize the particular discoveries of the previous chapters. The right to privacy and personal data protection in EU suffers from the uncodified character of norms. Reasons can be found in the historical evolution of the European integration.

1. Úvod

Je banálním faktem, že objem osobních údajů „shromážditelných“ a shromážděných roste úměrně zvyšování možností informačních technologií a „komputerizací“ všech lidských činností. Přestože legislativa na ochranu osobních údajů obsahuje technologicky neutrální terminologii, rozvoj technologií změnil kontext zejména pro právo subjektu osobních údajů na přístup k informacím. Tak je dnes usnadněna možnost subjektů osobních údajů kontrolovat, jaké údaje o nich jsou uchovávány, k čemu byly použity, přesnost údajů a zákonnost jejich zpracování. V nedávné minulosti kupř. zaměstnavatel (míněn běžný zaměstnavatel v demokratickém státě) neevidoval o zaměstnanci o mnoho více než adresu, údaj o druhu a místu výkonu práce, dni nástupu a záznamy o výplatách mzdy. Dotazy subjektů osobních údajů tak byly neobvyklé, a to se zřetelem k předvídatelnosti a omezenému množství uchovávaných údajů. Oproti tomu, dnes je příchod na pracoviště zaznamenáván na CCTV, vstup přes turniket nebo do výtahu pomocí elektronické karty, jakož i přihlášení se k počítači jsou evidovány. Uchovávány jsou provozní údaje o používání počítače. Tím by se také mělo zvyšovat množství dotazů. Stojí za poznamenání, že tento úsudek obстоjí jen tehdy, pokud odhlédneme od protichůdného hlediska spočívajícího v nezájmu o vyvolávání pozornosti zaměstnavatele. Zaměstnavatel je povinen sdělit všechny údaje, které o zaměstnanci uchovává. Uvedené ale může vyvolat problémy. Zaměstnanec zhusta zasílá tisíce e-mailů ročně, které mohou být uchovávány zaměstnavatelem na jeho serveru, přičemž některé z nich obsahují osobní údaje. Identifikovat mezi nimi takové může být enormně náročné. Úřady pro ochranu osobních údajů členských států zpravidla nepřipouští, aby se zaměstnavatelé zhostili svých povinností tím, že jednoduše stáhnou soubory z centrální databáze... úkoly zpracovatelů údajů jsou tak nesrovnatelně složitější, časově náročnější a nákladnější než v minulosti.

Příspěvek se zabývá transparentností ve zpracovávání osobních údajů. Jak uvádějí Bainbridge a Pearce, k dosažení transparentnosti mají přispět zejména: a) Právo subjektu osobních na přístup k údajům v držení zpracovatele. Přístup může být chápán i jako

předpoklad pro to, aby existovala možnost opravit chybné údaje. b) Právo subjektu údajů být podrobně informován o jejich zpracování.¹ Jinak řečeno, konstitutivní podmínku zákonnosti zpracování osobních údajů představuje přístup subjektu údajů k informacím o těchto – jeho se týkajících – procesech. S ním se úzce pojí možnost opravy údajů tak, aby byly správné, aktuální a relevantní k deklarovaným účelům. Pouze při splnění těchto požadavků zpracování osobních údajů nezakládá porušení oprávněných zájmů subjektů údajů.

2. Přístup subjektu údajů k informacím a právo na opravu osobních údajů v pramenech práva lidských práv

V platném primárním právu Evropské unie nejsou odpovídající nároky obsáhleji zakotveny a dovozovat je lze především z obecných právních zásad evropského práva.

Lisabonská smlouva (Návrh Smlouvy pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství), k jejímuž vypracování udělila mandát Evropská rada na zasedání konaném v Bruselu dne 21. a 22. 6. 2007, schválená v konečném znění dne 19. 10. 2007 Evropskou radou na zasedání v Lisabonu se záměrem její ratifikace do poloviny roku 2009, má změnit článek 6 odst. 1 Smlouvy o EU tak, že Unie uznává práva, svobody a zásady obsažené v Chartě základních práv Evropské unie, jež má stejnou právní sílu jako smlouvy.

Charta základních práv Evropské unie v čl. 8 odst. 1 až 3 stanoví, že každý má právo na ochranu osobních údajů, které se ho týkají, přičemž tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má

¹ Bainbridge, David, Pearce, Graham: 'Tilting the Windmills – Has the New Data Protection Law Failed to Make a Significant Contribution to Rights of Privacy'. *Journal of Information, Law and Technology*, 2000(2)

právo na jejich opravu. Na dodržování těchto pravidel dohlíží nezávislý orgán.

Všechny členské státy Evropské unie jsou smluvními stranami Úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluva“), přičemž ratifikace uvedeného aktu představovala právní podmínku přistoupení k Evropským společenstvím. Článek 6 Smlouvy o EU v účinném znění deklaruje, že Unie respektuje základní lidská práva, která zajišťuje Úmluva.

Úmluva o ochraně lidských práv a základních svobod zakotvuje ve svém čl. 8, že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Státní orgán přitom nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Byť se ze samotné dikce čl. 8 Úmluvy právo na přístup k informacím a právo na opravu osobních údajů nepodává, z judikatury Evropského soudu pro lidská práva odpovídající nároky s jistotou dovozovat lze.

3. Přístup subjektu údajů k informacím a právo na opravu osobních údajů v mezinárodních a evropských pramenech ochrany osobních údajů

V této souvislosti představují relevantní prameny zejména následující dokumenty. Zaprvé jde o Pravidla ochrany soukromí a přeshraničních toků osobních údajů (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) vydaná OECD 17. 9. 1980 (dále jen „Pravidla OECD“)². Další je Úmluva č. 108 na ochranu osob se zřetelem na automatizované zpracování osobních údajů (dále jen „Úmluva č. 108“), kterou přijala Rada Evropy 28. 1.

² Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, dostupné z http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html

1981.³ Konečně jde o Směrnici 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“).⁴

Uvedené právní akty predisponují obsah právních předpisů vydávaných evropskými státy, ať již prostřednictvím povinnosti transpozice jako je tomu v případě DPD, nebo alespoň coby zdroj inspirace.

Z „mimoevropských“ pramenů stojí za pozornost poměrně nedávno – v listopadu 2004 – na setkání ministrů APEC v Santiago de Chile schválený „Privacy Framework“.⁵

Možnost přístupu subjektu údajů k informacím a právo na opravu osobních údajů bývají též souhrnně označovány coby princip participace a kontroly subjektu údajů (principle of data subject participation and control).

Prvně jmenovaná „**zásada práva na přístup**“ (principle of the right of access) bývá též nazývána zásadou průhlednosti (principle of transparency) či otevřenosti (openness principle).⁶ Podle ní musí každé osobě 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.

Omezení vyplývajících práv je možné jen zákonem, který odpovídá příslušným lidskoprávním standardům. Z logiky věci je technicky nejobtížnější realizace této zásady v případě přenosu dat přes hranice nebo v případě mezinárodně sdílených databází.

Zásada je vyjádřena v čl. 8 písm. a) a b) Úmluvy č. 108. V DPD souvisí zejména s ustanoveními v čl. 7 písm. a), čl. 8 odst. 2 písm. a)

³ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, dostupné z <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

⁴ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

⁵ APEC Privacy Framework, dostupné z http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html

⁶ Z hlediska právní teorie se jakožto sporné jeví označovat „právo“ za „zásadu“.

a čl. 10-12. Zásada otevřenosti a právo na participaci jsou vyjmenovány jako šestý, respektive sedmý princip Pravidel OECD.

Do určité míry specifickým je princip článku 15 DPD zakazující rozhodnutí, které se významným způsobem dotýká subjektu, jen na základě automatizovaného zpracování údajů.

Uvedené se zrcadlí i v dokumentu APEC Privacy Framework coby princip VIII „přístup a oprava“. Jak podotýká Graham Greenleaf, přístup a oprava jsou zde formulovány explicitněji než v případě Pravidel OECD.⁷ Rámec APEC přitom zahrnuje několik výjimek: (i) náklady nebo výdaje jsou nepřiměřené ve vztahu k rizikům pro soukromí, (ii) je to nezbytné pro ochranu zákonnosti, bezpečnosti nebo obchodního tajemství, (iii) může být narušeno soukromí jiných osob. Tyto výjimky jsou formulovány široce a nezdá se, že by na ně (s výjimkou první) dopadal princip proporcionality. Nicméně podle Rámce APEC by jednotlivci měli mít právo na přezkum odmítnutí přístupu. Riziko uchovávání nesprávné informace je větší tam, kde je zamezeno přístupu uplatněním výjimky, Rámec APEC se však nezabývá tím, jaký je vztah mezi právem na přístup k údajům a právem na jejich opravu.

Druhá zásada inkorporuje **právo na opravu a výmaz** (principle of the right of rectification and erasure). Zásada je obsažena v člancích 5 písm. d) a 8 písm. c) Úmluvy č. 108. Článek 14 písm. b) DPD vymezuje právo dotčené osoby uplatnit odpovídající námitku.

Osobní údaje, které jsou předmětem automatizovaného zpracování, musí být přesné a – pokud je to potřebné – aktualizované.

Každé osobě musí být umožněno docílit, podle povahy případu, opravy předmětných údajů nebo jejich vymazání, jestliže jejich zpracování probíhá v rozporu s právními normami.

Obecně platný imperativ, dle kterého mohou být zpracovávány pouze pravdivé, přesné a aktuální údaje, není možné aplikovat bez ohledu na konkrétní souvislosti. I nepřesné nebo nepravdivé údaje mají nepochybný význam - např. v soudním spise. Zde jsou možnosti

⁷ Greenleaf, Graham.: APEC's privacy framework sets a new low standard for the Asia-Pacific, s. 103, in Kenyon, Andrew, Richardson, Megan: New Dimensions in Privacy Law. International and Comparative Perspectives. Cambridge University Press, Cambridge, 2006.

realizace práva na opravu nebo výmaz omezené, jak se podává kupř. z usnesení českého Ústavního soudu ze dne 24. 7. 2008, sp. zn. III. ÚS 274/07. Obecně však platí, že prohlášení subjektu údajů o nepravdivosti údaje a požadavku na jeho změnu nebo vymazání by mělo být uchováno ve spise, a to i bez jeho realizace v samotném datovém souboru.

4. Přístup k údajům a právo na opravu podle čl. 8 Úmluvy v judikatuře orgánů Úmluvy

Významným rozhodnutím týkajícím se práva na přístup k osobním údajům je rozsudek Evropského soudu pro lidská práva (dále jen „ESLP“, popř. „Soud“) ve věci *Gaskin v. Spojené království*.⁸ Zde stěžovatel brojil proti postupu Rady města Liverpool, která mu odmítla vydat důvěrné záznamy z období, kdy se nacházel v ústavní výchově. Rada dala najevo, že přístup k údajům by povolila jen v případě souhlasu toho, kdo údaje poskytl. Podle ESLP osoby ve stěžovatelově situaci mají „životní zájem chráněný Úmluvou“ na získání informací nezbytných k porozumění svému dětství a ranému vývoji. Na tomto podkladě se ESLP vyslovil, že k porušení čl. 8 Úmluvy došlo.

Není pochyb, že v kolizi s principem transparentnosti může stát ochrana třetích osob. Britská úprava, která zpřístupnění údajů podmiňovala souhlasem přispěvatele, je podle Evropského soudu pro lidská práva v zásadě souladná s čl. 8 Úmluvy. Tento systém však musí poskytovat adekvátní ochranu subjektu osobních údajů v situacích, kdy je osoba, která poskytla údaje, nedostupná nebo svévolně odmítá souhlas udělit. V tomto případě se tedy požaduje možnost přezkumu nezávislým orgánem, čemuž britská úprava nedostála.

ESLP zajištění práva na přístup k informacím ve věci *Gaskin* formuloval jakožto pozitivní závazek státu. Podle ESLP tedy nešlo o zásah do stěžovatelova práva na ochranu soukromí ve smyslu čl. 8 odst. 1 Úmluvy, ale o porušení pozitivních závazků chránit tato práva. Rozsah pozitivních závazků smluvního státu v této oblasti

⁸ Rozsudek Evropského soudu pro lidská práva ze dne 7. 7. 1989 ve věci *Gaskin v. Spojené království*, stížnost č. 10454/83.

vymezil ESLP následovně: 1/ musí být nastolena férová rovnováha mezi zájmy společnosti a zájmy jednotlivce, 2/ musí být vzaty v potaz meze uvážení (margin of appreciation) státu, je-li tato rovnováha porušena a 3/ cíle obsažené v čl. 8 odst. 2 musejí dosáhnout určité relevance.

Právo na přístup k informacím ale nezahrnuje všechny druhy osobních údajů. Ve věci Gaskin ESLP deklaroval, že pro existenci práva na přístup k údajům představuje význam informace pro jednotlivce podmínku nutnou, nikoli dostačující.

Tento předpoklad se zvláště zřetelně uplatnil – již dříve – ve věci Leander, kde ESLP konstatoval, že švédské úřady neměly povinnost poskytnout stěžovateli údaje, na jejichž podkladě mu byl odepřen přístup k zaměstnání.⁹

Po rozsudku Gaskin následovalo několik závažných rozhodnutí týkajících se přístupu k informacím.

Prvním z nich byl rozsudek ve věci McMichael v. Spojené království.¹⁰ V této věci byli stěžovateli rodiče dětí, které jim státní orgány odňaly z opatrování a svěřily do ústavní výchovy. Vytýkali, že se nemohli seznámit s obsahem některých dokumentů, z nichž rozhodnutí vycházelo. ESLP konstatoval porušení čl. 8 odst. 1 Úmluvy, byť formálně vzato, byl účastníkem opatrovnického řízení jen jeden ze stěžovatelů. ESLP přitom neshledal podstatným, zda odpovídající právo na přístup k údajům zajišťuje rovněž čl. 6 Úmluvy.

Další je rozsudek ve věci Guerra a ostatní v. Itálie.¹¹ Zde se ESLP vyslovil, že státní orgány zanedbaly splnění určitých zákonných závazků týkajících se informování obyvatel města o vážných ekologických rizicích, čímž se zároveň dopustily porušení pozitivního závazku chránit soukromý a rodinný život podle čl. 8 Úmluvy. Rozhodnutí znamená, že státní orgány jsou v některých případech povinny informovat veřejnost bez ohledu na to, zda jsou o sdělení požádány. Toto rozhodnutí je hodno pozornosti rovněž proto,

⁹ Rozsudek Evropského soudu pro lidská práva ze dne 26. 3. 1987 ve věci Leander v. Švédsko, stížnost č. 9248/81.

¹⁰ Rozsudek Evropského soudu pro lidská práva ze dne 24. 2. 1995 ve věci McMichael v. Spojené království, stížnost 16424/90.

¹¹ Rozsudek Evropského soudu pro lidská práva ze dne 19. 2. 1998 ve věci Guerra a ostatní v. Itálie, stížnost č. 116/1996/735/932

že právo na přístup k informacím má širší dosah, než tomu bylo v případě rozhodnutí Gaskin. Ve věci Gaskin ESLP judikoval jen právo na informace nezbytné k porozumění stěžovatelu „dětství a ranému vývoji“. V odůvodnění rozsudku Guerra ESLP konstatoval, že pod čl. 8 Úmluvy mohou spadat též informace „neosobní“ povahy, které však jsou způsobilé ovlivnit zdravotní stav osob, a to přinejmenším tehdy, pokud je jejich zdraví vážně ohroženo. Článek 8 Úmluvy tedy může představovat východisko nejen pro ochranu osobních údajů, ale taktéž pro přístup k informacím obecně.

Ve věci McGinley a Egan v. Spojené království se ESLP přidržel linie nastolené v rozsudku Guerra a konstatoval, že státní orgány, do jejichž pravomoci spadají nukleární testy, jsou podle čl. 8 Úmluvy povinny ustavit účinné a dostupné („effective and accessible“, srov. odst. 101) postupy umožňující občanům vyhledat všechny relevantní informace o dopadech testování na jejich zdraví.¹²

Ve věci Martin v. Spojené království Evropská komise pro lidská práva (dále jen „EKLP“, popř. „Komise“) konstatovala soulad s čl. 8 Úmluvy, pokud šlo o úpravu podmiňující přístup k lékařským záznamům vyjádřením lékaře, že tím nemůže být poškozen pacient nebo jiné osoby.¹³ V daném případě se stěžovatel neúspěšně domáhal přístupu k údajům ohledně jeho psychiatrické léčby, kterou zahájil v devatenácti letech a trvala čtyři roky. Komise konstatovala, že oproti případu Gaskin se záznamy netýkají období dětství a nejde o jedinou cestu, jak získat informace o době, kdy postupoval psychiatrickou léčbu. Komise shledala, že řízení sleduje legitimní cíl aprobovaný čl. 8 Úmluvy – ochranu zdraví. Komise poznamenala, že záznamy nebyly požadovány k lékařským účelům ani pro právní řízení a stěžovatel si mohl sám určit lékaře, který vybere údaje vhodné ke zpřístupnění. Komise dala najevo, že tato úprava ustavuje férovou rovnováhu mezi uvedeným legitimním cílem a stěžovatelovým požadavkem na přístup k údajům. Stížnost byla proto shledána nepřijatelnou.

¹² Rozsudek Evropského soudu pro lidská práva ze dne 9. 6. 1998 ve věci McGinley a Egan v. Spojené království, č. 10/1997/794/995-996

¹³ Rozhodnutí Evropské komise pro lidská práva ze dne 28. 2. 1996 ve věci Martin v. Spojené království, stížnost č. 27533/95

Omezené právo na přístup k informacím může být dovozováno z čl. 10 Úmluvy. Tento článek Úmluvy zakazuje státu, aby bránil osobě přijímat informace, které jí ostatní chtějí poskytnout. Na druhou stranu čl. 10 bez dalšího nezaručuje osobám přístup do úředních rejstříků obsahujících záznamy o nich. Tento výklad byl ESLP potvrzen ve věci Gaskin.

Rozsudky ve věcech Leander a Gaskin ale není správné interpretovat tak, že z čl. 10 Úmluvy nemůže vyplývat právo na přístup k informacím uchovávaným státními orgány.

V obou případech se totiž jednalo o situaci, kdy se žadatel domáhal přístupu k záznamům vedeným o jeho osobě, a tedy majícím význam specificky pro něj samotného.

Zájem veřejnosti zde ve hře nebyl. Pokud by se Gaskin domáhal přístupu k informacím o jednání orgánů sociální péče vůči více osobám, byl by poukaz na čl. 10 Úmluvy výstižný.

Tento předpoklad není vyvrácen ani rozsudkem ve věci Guerra, kdy veřejné orgány opomenuly poskytnout (ze své vlastní iniciativy) informace o ekologických rizicích a ESLP se nevyslovil, že tím porušily čl. 10 Úmluvy. Soud totiž neformuloval závěr, že by smluvní stát svým závazkům podle čl. 10 Úmluvy dostal, pokud by kupř. zamítl žádost o poskytnutí informace obdobné povahy.

Ve věci Chave née Jullien stěžovatelka napadla postup státních orgánů, které odmítly vymazat záznamy o její nezákonné detenci v psychiatrické léčebně.¹⁴ Komise dospěla k závěru, že pokračující uchovávaní sporných záznamů státními orgány je v souladu se zákonem a nezbytné v demokratické společnosti k ochraně zdraví. Nicméně Komise konstatovala, že pod čl. 8 odst. 1 Úmluvy spadá i právo na opravu a vymazání údaje.

Spory týkající se práva na opravu a vymazání údaje často vycházejí z činnosti státních orgánů, které zamítají odpovídající žádosti transsexuálů. Komise v těchto případech poukazuje na čl. 8 odst. 1 Úmluvy, hovoří o tom, že tyto údaje jsou způsobilé „determinovat“ jejich „sexuální identitu“. Soud je poněkud konzervativnější. Ve věcech Rees v. Spojené království a Cossey v. Spojené království neshledal porušení čl. 8 Úmluvy v postupu

¹⁴ Rozhodnutí Evropské komise pro lidská práva ze dne 9. 7. 1991 ve věci Chave née Jullien, stížnost č. 14461/88

britských úřadů, které odmítly provést změnu v údaji o pohlaví v rodných listech stěžovatelů.¹⁵ Soud dovodil, že by podobné „adjustace“ mohly vést k příliš rozsáhlé změně v systému matričních záznamů a vyvolat problematické následky pro právní jistotu ostatní populace. Soud zdůraznil, že smluvní státy disponují širokým prostorem k úvaze (margin of appreciation), pokud jde o uznání právního statusu transsexuálů, což je dáno neexistencí „společného základu“ mezi smluvními státy v této oblasti. Soud rovněž podotkl, že transsexuálové ve Spojeném království si mohou změnit jméno a příjmení a údaj o pohlaví obsažený v rodném listu není převzat do mnoha dalších oficiálních dokumentů. Ve věci B v. Francie ESLP lišil od případů Rees a Cossey, jelikož pozici transsexuálů ve Francii shledal co do administrativních překážek obtížnější než ve Spojeném království.¹⁶

Ve zmiňovaných případech ESLP zdůraznil pozitivní závazky smluvních států vyplývající z čl. 8 odst. 1 Úmluvy na úkor konstatování, že v daných případech došlo k zásahu do čl. 8 odst. 1 Úmluvy. Z hlediska Soudu „pouhé odmítnutí“ smluvního státu opravit úřední záznamy nemůže znamenat zásah. Soud neshledal nezbytným aplikovat čl. 8 odst. 2 Úmluvy. Zmínil se však (v souvislosti s věcí Gaskin), že cíle zmiňované v čl. 8 odst. 2 Úmluvy mají význam, pokud jde o vyvažování zájmů společnosti a jednotlivce.

Judikatura formulovala závěr, že čl. 8 odst. 1 Úmluvy poskytuje určitou ochranu zájmu jednotlivce na přístup k údajům uchovávaným o něm samém ostatními. Čl. 8 odst. 1 Úmluvy ale neposkytuje právo na participaci jednotlivce, respektive právo na přístup k informacím v širokém smyslu. Oproti tomu, zákony na ochranu osobních údajů toto právo zakotvují. Právo na přístup k informacím však není absolutní, ale závisí rovněž na tom, jaký význam má údaj pro jeho subjekt. V praxi však rozdíl mezi imperativy odvíjejícími se z čl. 8 Úmluvy a zákonů na ochranu osobních údajů není velký. Současně

¹⁵ Rozsudek Evropského soudu pro lidská práva ze dne 17. 10. 1986 ve věci Rees v. Spojené království, stížnost č. 9532/81, rozsudek Evropského soudu pro lidská práva ze dne 27. 9. 1990 ve věci Cossey v. Spojené království, stížnost č. 10843/84

¹⁶ Rozsudek Evropského soudu pro lidská práva ze dne 25. 3. 1992 ve věci B. v. Francie, stížnost č. 13343/87

jde čl. 8 Úmluvy v některých případech dále a dopadá i na „neosobní“ údaje, zejména ty, které mohou osvětlit závažná zdravotní rizika.

5. Přístup k údajům a právo na opravu v právu členských států Evropské unie

5. 1. Rámec ustavený DPD a stupeň dosažené konvergence

DPD vychází z návrhu Evropské komise z roku 1990, přičemž poprvé zařadila pod dosah ochrany osobních údajů některé manuálně („nepočítačově“) zpracovávané soubory informací. Čl. 95 SES limituje použitelnost DPD na oblast prvního pilíře. Oproti tomu, Úmluva č. 108 podobnému omezení nepodléhá a byla ratifikována všemi smluvními státy Rady Evropy.

Problematika přístupu k osobním údajům otevírá řadu otázek, jako kupř. kolik informací poskytnout, zda může být uložen „rozumný“ poplatek, nebo zda některé informace mohou být upraveny (kupř. tehdy, pokud poskytnuté informace obsahují též údaje o třetích osobách). Osobní údaje mohou být obsaženy v množství databází umístěných v různých zeměpisných oblastech nebo delokalizovaných, v důsledku čehož může být složité nalézt všechny osobní údaje, kterých se jejich subjekt dožaduje.

DPD zakotvuje obecné principy práva být informován a práva na přístup k osobním údajům. Ponechává přitom mnoho implementačních detailů na členských státech. Článek 12 DPD poskytuje subjektům osobních údajů právo obdržet určité základní informace od zpracovatele osobních údajů o procesu jejich zpracování. Zatímco čl. 12 výslovně zaručuje pouze to, že „bez omezení v rozumných intervalech a bez excesivní lhůty nebo výdajů“ bude zajištěn výkon práv obsažených pod písm. a) (potvrzení, sdělení a oznámení), v praxi se všeobecně uznává, že tyto podmínky dopadají i na výkon práv obsažených pod písm. b) a c) (opravu, výmaz nebo blokování údajů, oznámení třetí osobě).

DPD poskytuje jednotlivcům další související práva, kupř. v čl. 14 právo uplatnit námitky proti zpracování osobních údajů, resp.

v čl. 15 právo nebýt podřízen „automatizovaným individuálním rozhodnutím“. Zmiňované právo uplatnit námitky proti zpracování osobních údajů musí být interpretováno extenzívně. Automatizované rozhodnutí je definováno jako to, co zakládá právní účinky týkající se subjektu osobních údajů nebo podstatně ho ovlivňující a které vychází z výhradně automatizovaného zpracování dat se záměrem hodnotit některé osobní aspekty vztahující se k němu, jako kupř. výkon v práci, schopnost splácet úvěry, spolehlivost apod. Příkladem automatizovaného rozhodnutí může být kupř. takové, kterým se na základě numerických kritérií – bez zásahu člověka – odepře poskytnutí úvěru. Kvůli snížení rizik vyplývajících z tohoto postupu v praxi rozhodovací proces – tak jako tak – finalizuje člověk.

Je zřejmé, že samotný proces vyhledávání těchto uchovávaných osobních údajů kupř. za účelem jejich výmazu nebo zablokování může představovat riziko jejich prozrazení.

Evropská komise shledala, že úroveň harmonizace práva na přístup k osobním údajům je „uspokojivá“, ale mezi státy existují podstatné rozdíly.¹⁷

Následující text se zabývá jednak normativními, jednak judikatorními otázkami konvergence ochrany osobních údajů v členských státech Evropské unie.

5. 2. Normativní otázky konvergence ochrany osobních údajů v členských státech Evropské unie

Ze studie *The Data Subject's Right of Access and to be Informed in Finland: An Experimental Study*, jejímž autorem je Mika Raento, mapující implementaci DPD se podává, že rovněž ve Finsku přetrvávají některé problémy, pokud jde o získání přístupu k údajům a ověřování správnosti poskytnutých informací.¹⁸

¹⁷ European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States 20.

¹⁸ Raento, Mika: *Data Subject's Right of Access and to be Informed in Finland: An Experimental Study*. *International Journal of Law and Information Technology*, 2006, Vol. 14, No. 3, s. 390.

Studii podobnou finské vypracoval ve Spojeném království Department for Constitutional Affairs v roce 2003.¹⁹ V rámci tohoto výzkumu byli respondenti dotazováni, zda narazili na problémy při získávání informací, které požadovali. Ti, kteří odpověděli kladně, většinou poukazovali na neochotu zpracovatelů osobních údajů přiznat, že tyto údaje uchovávají, a dobu potřebnou ke získání údajů.

Lze zobecnit, že zákony o ochraně osobních údajů vydané v členských státech Evropské unie stojí na třech východiscích:

- a/ Ochrana osobních údajů, jakožto základního práva zaručeného ústavněprávními normami.
- b/ Ochrana soukromí jako lidského práva zakotvené v Úmluvě č. 108.
- c/ Článek 95 (ex-čl. 101a) Smlouvy o založení ES a z něj se odvíjející DPD.

Zákony o ochraně osobních údajů členských států úzce reflektují DPD, zejména pokud jde o koncept informovaného souhlasu, právo být informován a právo na přístup k údajům. Bývají přitom aplikovány i mimo dosah otázek souvisejících s vnitřním trhem.

Zákony o ochraně osobních údajů definují, jaké údaje musí zpracovatel osobních údajů poskytnout. Zpracovatel tak je povinen ke každému souboru údajů stanovit účel zpracování a druh zpracovávaných údajů. Tyto specifikace musejí být veřejně dostupné.

Namísto je poskytnout i další informace; zákony ukládají zveřejnit přesný kontakt na zpracovatele osobních údajů, popis subjektů, pro něž jsou tyto soubory určeny, komu budou osobní údaje předány a popis principů zajištění datové bezpečnosti.

Popis souboru musí být dostupný veřejnosti. Zpracovatel je povinen poskytnout všechny tyto informace subjektům osobních údajů již ve fázi sběru osobních údajů. Navíc zpracovatel osobních údajů musí informovat subjekt osobních údajů o právu na přístup k údajům a na opravu údajů.

Požadavek informovat dohledový úřad v některých případech neuplatní, zejména tehdy, je-li patřičná informace již veřejně dostupná. Uvedené řešení lze pokládat za racionální.

¹⁹ Response to the Consultation Paper Data Protection Act 1998: Subject Access July 2003. Dostupné z <http://www.dca.gov.uk/consult/foi/dpsaresp.htm>.

Ne ve všech členských státech ale zákony o ochraně osobních údajů stanoví, že subjekt osobních údajů má právo požadovat informaci o zdroji těchto údajů, účelu shromažďování, resp. použití údajů a jejich poskytnutí třetím stranám.

Zákony o ochraně osobních údajů omezují právo na přístup k osobním údajům typicky v následujících situacích:

- poskytnutí přístupu k údajům by ohrozilo národní bezpečnost, obranu, veřejný pořádek, bezpečnost, prevenci nebo vyšetřování trestných činů,
- poskytnutí přístupu k údajům by mohlo představovat vážné nebezpečí pro zdraví nebo léčbu subjektu osobních údajů nebo někoho dalšího,
- jestliže údaje jsou používány výhradně pro historické, vědecké nebo statistické účely,
- jestliže je neposkytnutí údajů nezbytné pro zabezpečení významného ekonomického nebo finančního zájmu státu nebo Evropské unie.

I v těchto případech je však třeba na žádost o poskytnutí osobních údajů reagovat a dát najevo, že je založen důvod pro odepření přístupu. Bez významu nemusí být, že některé zákony zakotvují, že lze požadovat poskytnutí údajů v listinné (a contr. elektronické) podobě a formou písemné žádosti. Kupříkladu finské právo neukládá zpracovateli osobních údajů, aby uvedl, jak dlouho jsou uchovávány údaje o peněžních transakcích – zahrnující osobní údaje – a není tak možné se ujistit, zda zpracovatel údaje skutečně uchovává či nikoli. Pouze lucemburské právo požaduje, aby byla délka uchovávání uvedena.²⁰ Minimální dobu, po kterou musejí být údaje uchovávány, stanoví finské účetní právo, a to v délce 10 let. Tyto údaje samozřejmě mohou být transformovány do podoby, v níž nepodléhají zákonu o ochraně osobních údajů (ručně vedené záznamy řazené pouze podle časové návaznosti). Mika Raento upozorňuje, že banky nepovažují údaje o výplatách mezd,

²⁰ Korff, Douwe: EC Study on Implementation of Data Protection Directive. (Comparative Summary of National laws), s. 100. Dostupné z http://www.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

bankovních transakcích, platebních příkazech a výkazech za osobní údaje. Banky pokládají za osobní údaje jen ty, které představují základní údaje o zákazníkovi. To podle autora samozřejmě nemá podkladu v právní úpravě.²¹ Autor dále uvádí, že tam, kde banky poskytly údaje o transakcích formou výpisů z účtů a ročních zpráv, již obecně nemají povinnost učinit tak znovu. Není rovněž zcela jasné, jak vykládat pojem „jednou ročně“: musejí zpracovatelé zaslat údaje, které nebyly poskytnuty v průběhu uplynulého roku? Poukazuje, že švédský úřad pro ochranu osobních údajů rozumně dovedl, že pokud subjekt osobních údajů je průběžně zpravován, může se ve své odpovědi omezit na poukaz na tuto okolnost.

Zvláštní pozornost si zasluhují náklady vynaložené na poskytnutí informace. Zpracovatelé osobních údajů namítají, že poskytování přístupu může být spojeno s vysokými náklady.²² Někteří respondenti v britské studii tvrdili, že zodpovězení jediného dotazu si může vyžádat náklady přes 1.000 britských liber.²³ Zpracovatelé označili „vystopování“ všech relevantních údajů za jeden z hlavních problémů v rámci poskytnutí odpovědi. K tomu srov. preambule DPD, bod 46. Na druhé straně švédský nebo německý zákon o ochraně osobních údajů umožňují přístup k osobním údajům bezplatně. Ve Finsku je možný bezplatný přístup k údajům jen jedenkrát ročně, ve Velké Británii zpracovatel může uložit poplatek nad 10 liber za zpřístupnění a mezi žádostmi o přístup musí uplynout rozumná doba (Data Protection Act 7 (2) (b)). Podobně v českém zákoně č. 101/2000 Sb., o ochraně osobních údajů, s refundací nákladů správce osobních údajů vzniklých poskytnutím informace počítá § 12 odst. 3.

Tyto rozdíly mohou vyvolávat problémy pro zpracovatele osobních údajů, kteří zpracovávají osobní údaje pocházející

²¹ Raento, Mika: Data Subject's Right of Access and to be Informed in Finland: An Experimental Study. *International Journal of Law and Information Technology*, 2006, Vol. 14, No. 3, s. 402.

²² Korff, Douwe: EC Study on Implementation of Data Protection Directive. (Comparative Summary of National laws), s. 107. Dostupné z http://www.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

²³ Response to the Consultation Paper Data Protection Act 1998: Subject Access July 2003. Dostupné z <http://www.dca.gov.uk/consult/foi/dpsaresp.htm>.

z různých členských států, a představovat tak překážku intrakomunitárního obchodu tím více, že její efekt mohou navýšit náklady měnové konverze.

Za zmínku stojí otázka informačních systémů podniků i orgánů veřejné správy, které by měly předdefinovanou funkci vyhledání uchovávaných osobních údajů. Evropská komise se v této souvislosti vyslovila pro podporu technologií zlepšujících soukromí zaměřených na anonymitu a pseudonymitu.²⁴ Tento SW by zahrnoval i facility označující ty uchovávané údaje, které mají osobní povahu. Facility mají zajistit plnění závazků vyplývajících z transpozice směrnice DPD, jako kupř. omezení předávání osobních údajů třetím subjektům nebo omezení uchovávání údajů na dobu nezbytnou pro původní účel. Jedním z těchto programů je Tivoli Privacy Manager společnosti IBM.

5. 3. Judiciální otázky konvergence ochrany osobních údajů v členských státech Evropské unie

5. 3. 1. Případ Durant v. Financial Services Authority

Z hlediska judiciálního výkladu práva na přístup k subjektu údajů k informacím a práva na opravu osobních údajů představuje významný mezník rozsudek britského Odvolacího soudu ze dne 8. 12. 2003 ve věci Durant v. Financial Services Authority, No. B2/2002/2636, kterým byly formulovány klíčové koncepty ochrany osobních údajů v britském právu.²⁵ Z pohledu tohoto článku je podstatné, že rozsudek byl předmětem diskuse mezi vládou

²⁴ European Commission, Internal Market DG (2003). Terms of reference of the technical workshop on Privacy-Enhancing Technologies organised by DG Internal Market on the 4th of July in Brussels. Dostupné z http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/pet/200304-pet-tor_en.pdf

²⁵ Durant v. Financial Services Authority, No: B2/2002/2636, dostupný z <http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm>

Spojeného království a Evropskou komisí co do svého souladu právem EU na ochranu osobních údajů.

Pan Durant (dále též „žalobce“) byl zákazníkem Barclays Bank. V roce 1993 prohrál svůj spor s touto bankou. Neúspěšně se pokusil o zpřístupnění údajů o něm vedených bankou za účelem obnovy řízení. V létě 2000 si stěžoval na banku u Úřadu pro finanční služby (Financial Services Authority, dále jen „FSA“). Dotázal se rovněž FSA, jaké dokumenty obdržela od Barclays ve své roli bankovního dohledu. FSA provedla šetření a věc uzavřela bez toho, že by žalobce informovala o jeho výsledku. Poukázala přitom na povinnost mlčenlivosti vyplývající z bankovní legislativy. Žalobce se obrátil se stížností k Stížnostnímu komisaři FSA (FSA Complaints Commissioner), ale tento jeho návrh byl zamítnut.

V září a říjnu 2001 žalobce vznesl dva podněty ohledně údajů k FSA podle § 7 DPA za účelem zpřístupnění počítačových a manuálních záznamů. FSA poskytla kopie dokumentů uchovávaných v elektronické podobě, z některých byly přitom odstraněny údaje o třetích osobách. FSA odmítl žádost o zpřístupnění manuálních záznamů s vysvětlením, že se nejedná o osobní údaje ve smyslu § 1 odst. 1 britského zákona o ochraně údajů (Data Protection Act, dále jen „DPA“), jelikož netvořily součást „relevant filing system“ (relevantního systému souborů). Žalobce se bezúspěšně obrátil postupem podle § 7 odst. 9 DPA ke County Court s tvrzením, že FSA porušil jeho právo na přístup k informacím. Poté se odvolal k Odvolacímu soudu, kde byl opět neúspěšný. Odvolací soud podstatně omezil právo na přístup k údajům ve věci Durant v. Financial Services Authority tím, že zamítl návrh, kterým se žalobce domáhal přístupu k neupraveným počítačovým dokumentům a rukopisným záznamům uchovávaným Barclays Bank, a to na podkladě úsudku, že označené záznamy elektronické nelze kvalifikovat jako „osobní údaje“ a rukopisné nepředstavují „relevant filing system“ (relevantní systém souborů) ve smyslu britského práva ochrany osobních údajů.

V souvislosti se zamítnutím odvolání žalobce Odvolací soud vymezil čtyři základní otázky:

1/ které údaje (zda uchovávané v počítačových nebo manuálních souborech) jsou „osobní“ v tom smyslu, že spadají pod dosah práva na přístup k osobním údajům,

2/ co je „relevantní systém souborů“,

3/ zda zpracovatel osobních údajů má povinnost vyhovět žádosti o poskytnutí údajů tam, kde by tím došlo k předání osobních údajů o třetí osobě, s výjimkou případů, kdy je to „rozumné za všech okolností“,

4/ soud má pravomoc nařídit zpracovateli osobních údajů, který nesprávně odepřel přístup k údajům, aby předchozí žádosti vyhověl.

Dále bylo třeba pozornost obracet k otázce, jaké principy se přitom musí uplatnit.

5. 3. 2. Obsah pojmu osobní údaj

Osobní údaje jsou definovány jako „údaje, které se vztahují k žijícímu jednotlivci“ (living individual). Údaje mohou být uchovávány v počítačovém nebo manuálním souboru. Žalobce tvrdil, že pojem osobní údaj má široký rozsah a zahrnuje všechny informace, které jej identifikují, včetně kupř. dokumentace vytvořené FSA v souvislosti s vyšetřováním jeho stížností. FSA oponoval, že slova „vztahující se k“ jsou způsobilá zahrnout všechny informace od těch s přímou vazbou k jednotlivci po údaje s jen povšechnou vazbou k němu, a požadoval, aby byl přijat úzký výklad uvedeného pojmu.

Odvolací soud vzal za určující hledisko, zda jsou zpracovávané osobní údaje způsobilé zasáhnout do soukromí subjektu osobních údajů. Upozadil otázku, byl-li subjekt osobních údajů v souboru jmenován. Soud konstatoval, že pouhé zmínění jména jednotlivce neznamená, že jde o osobní údaj. Soud se k řešení otázky, zda jde o osobní údaj či nikoli, vyslovil tak, že určující je „kontinuum relevance nebo blízkosti k subjektu osobních údajů“, a nikoli jen k „transakcím nebo záležitostem, které se ho mohou ve větším nebo menším stupni týkat“.

Soud identifikoval dva pojmy, které mohou pomoci při určení, zda je údaj osobní. První je, zda informace byla „biografický v podstatném smyslu“. To znamená, že o osobní údaj nejde tam, kde nejsou „osobní konotace“ nebo „soukromé implikace“. Zadruhé, o osobní údaj půjde tehdy, když se soustřeďuje na určitou osobu spíše, než aby tento subjekt osobních údajů byl jen zmiňován a primárně se datový soubor soustřeďoval na osobu jinou nebo určitou událost.

Soud tak konstatoval, že „je to informace, která ovlivňuje jednotlivcovo soukromí, ať již v oblasti osobního nebo rodinného života, obchodní nebo profesní činnosti.

Koncept osobních údajů je nesporně základem legislativy na ochranu osobních údajů. Jestliže je údaj „osobní“, jeho zpracovateli vznikají povinnosti, které musí splnit, a naopak. Je tedy významné, aby (potenciální) zpracovatel osobních údajů uměl rozlišit, zda o osobní údaj jde, či nikoli. Zákonný rámec vychází z předpokladu, že zpracovatel osobních údajů dovede rozlišit, kdy jde o osobní údaj.

Toto judiciální vymezení osobních údajů má však svá úskalí. Soud sice deklaroval snahu vytvořit řešení, které by umožňovalo, aby na žádost mohl reagovat „úředník bez zvláštní znalosti souborů nebo subjektu osobních údajů“, avšak ve skutečnosti je systém funkční jen v jednoduchých případech a v situacích složitějších vyžaduje znalost kontextu. Uvedenému ovšem nemůže běžně informovaný úředník dostát.

Pohled soudu na význam pojmu „osobní údaj“ značně omezuje ochranu poskytovanou i v jiných souvislostech, než je přístup k údajům. Pokud by byl názor obsažený v rozsudku ve věci Durant správný, zpracovatelé osobních údajů by mohli sbírat množství osobních informací „nezaměřených biograficky“ bez náležité právní ochrany.

Podle mého názoru by stačilo poukázat, že informace doposud nebyla použita v takovém kontextu, kdy se stává osobním údajem, pročez s ní lze nakládat prakticky libovolně. Tím ovšem ztrácí na významu zásada „férového zpracování informací“, která je konstitutivní součástí DPD. Jestliže se informace v rukou zpracovatele stane osobním údajem až v určité fázi, bude postačovat, aby před tímto kritickým bodem byla informace předána mimo dosah právních standardů EU/EHP – do některého z „datových rájů“.

Sporné je rovněž uvažovat o „biografičnosti v podstatném smyslu“ a „soustředěnosti na jednotlivce“ v obsáhlých elektronických databázích nebo v případě shromažďování počítačových údajů o použití čipových karet při vstupu na pracoviště a odchodu z něj a o uskutečněných telefonických hovorech. Zpracovatelé tak mohou údaje uchovávat primárně k obchodním nebo personálním účelům a být způsobilí vytvořit z nich (často ve vzájemné kombinaci) zprávy, které ovlivní jednotlivcovo soukromí.

Namíste by bylo volit kritéria s užšími hranicemi uvážení ze strany zpracovatelů dat.

Za zaznamenání stojí, že Odvolací soud odkazoval na recitál 15 DPD s tím, že se vztahuje na manuálně zpracovávané soubory. Ve skutečnosti recitál 15 je nutno aplikovat ve spojení s recitálem 14, přičemž odkazuje jen na zvukové a obrazové údaje. Nejde však o zásadní pochybení, neboť na recitál 15 se odkazuje v souvislosti s potřebou snadného přístupu k manuálním souborům a jejich strukturováním, přičemž recitál 27, na který rozhodnutí správně mělo odkazovat, je s recitálem 15 obsahově totožný.

5. 3. 3. Manuální soubory a legislativa na ochranu osobních údajů

Požadavek žalobce směřoval na manuální soubory zpracovávané FSA. Soud zvažoval, zda tyto soubory spadají pod dosah legislativy na ochranu osobních údajů. Vycházel z pojmu „relevantní systém souborů“ použitého v zákonné definici pojmu údaj. Relevantní systém souborů je každý soubor informací vztahující se k jednotlivci a (ačkoliv, jak vyplývá z logiky věci, není veden počítačově) je strukturován, ať již podle spojení k jednotlivcům nebo podle jiných kritérií, což umožňuje, aby specifická informace vztahující se k jednotlivci byla dostupná. Směrnice používá podobnou definici. Recitály směrnice zdůrazňují, že ochrana osobních údajů musí splňovat tytéž požadavky, ať již se jedná o soubory zpracovávané automaticky (počítačově) nebo manuálně, že manuální soubory musejí být strukturovány, aby byl umožněn jednoduchý přístup k osobním údajům a manuální soubory, které nejsou strukturovány nespádají do rozsahu směrnice.

Britský Odvolací soud se vyslovil, že směrnice má být ve vztahu k manuálním souborům interpretována restriktivně a že Parlament zamýšlel, aby DPA byla aplikována na manuální záznamy jen tehdy, pokud jsou tyto systémy „dostatečně sofistikované, aby poskytl stejný nebo podobný standard přístupnosti jako počítačové systémy.

Uzavřel, že „relevantní systém souborů“ je omezen na systém:

1/ ve kterém soubory tvořící jeho části jsou strukturovány nebo vztaženy takovým způsobem, že je jednoduché z výsledku vyhledávání určit, zda specifická informace je způsobilá nabýt

rozměru osobního údaje jednotlivce vznášejícího dotaz, zda jsou jeho osobní údaje uchovávány v systému a pokud ano, ve kterých souborech;

2/ přičemž systém je dostatečně sofistikovaný a podrobný, aby bylo možné indikovat zda a kde v jednotlivém souboru nebo souborech specifická kritéria nebo informace o jednotlivci mohou být snadno nalezeny.

FSA uchovávala různé soubory obsahující informace o žalobci, včetně dvou souborů nadepsaných „Mr Durant“ s dokumenty vztahujícími se k jeho stížnosti s listinami uspořádanými v chronologickém pořadí. Soud odmítl tvrzení, že jde o součást „relevantního systému souborů“, a ku podpoře tohoto závěru uvedl, že schopnost obsluhy identifikovat a lokalizovat soubory, včetně těch organizovaných chronologicky nebo jmenovitě, není dostatečná.

5. 3. 4. Komentář k termínu relevantní systém souborů

Přestože směrnice i DPA indikují, že manuální soubory spadají pod tuto úpravu jen tehdy, pokud jsou strukturovány tak, aby specifické informace bylo možno bez obtíží dohledat, ani směrnice ani DPA nestanoví, že manuální systémy musejí mít v tomto směru ekvivalentní parametry jako počítačové systémy. V této souvislosti lze poukázat na recitál 27 DPD, podle něhož musí být ochrana osobních údajů aplikována jak na jejich automatické zpracování, tak i na zpracování manuální. Požadavek na ekvivalenci vznesený Odvolacím soudem nejen postrádá normativní oporu, ale je i – ve složitějších případech – prakticky nerealizovatelný. Rozsah ochrany nesmí být neodůvodněně rozdílný v závislosti na použité technologii, jinak vzniká riziko obejítí úpravy. Je však pravda, že manuální systémy musejí být dostatečně strukturovány, aby se na ně vztahovala DPD.

Britský Komisař pro informace zveřejnil stanovisko, podle něhož je nutný test o dvou krocích.²⁶ Jeho první část se vztahuje ke znalosti

²⁶ The ‘Durant’ case and its impact on the interpretation of the Data Protection Act 1998 (2 February 2004). Dostupné z http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist

zpracovatele osobních údajů ohledně systému a hlavně jeho indexování. Jak se test použije, závisí na tom, zda informace jsou řazeny jmenovitě nebo tématicky. Jestliže jsou řazeny podle jména, zpracovatel údajů potřebuje vědět, že systém bude obsahovat kategorii požadovaných osobních údajů. Pokud je systém indexován podle vztahu k určitému předmětu, zpracovatel údajů potřebuje vědět, že systém je indexován tak, že je možné najít informaci o určitém jednotlivci. Jestliže manuální systém souborů naplňuje kritérium první části testu a soubory jsou rozčleněny nebo indexovány tak, že hledající osoba může nalézt požadovanou informaci bez manuálního hledání (tj. bez toho, že by postupně procházel všechny záznamy), spadá bez dalšího do kategorie relevantní systém souborů. Komisař zdůrazňuje, že podle jeho názoru systém souborů uspořádaných čistě chronologicky není „relevantním systémem souborů“. Jeho závěr je ten, že jen velmi málo manuálních souborů je podřaditelných režimu DPA. Na tomto podkladě lze konstatovat, že pod uvedený režim budou spadat jen ty nejorganizovanější osobní složky. Tímto názorem komisař zašel dokonce dále než Odvolací soud. Zatímco komisař konstatoval, že soubory uspořádané toliko chronologicky nejsou relevantním systémem souborů, Odvolací soud dal najevo, že chronologické uspořádání „není postačující“ pro uvedenou subsumpci.

V intencích této argumentace jen chronologicky řazené záznamy relevantním systémem souborů nebudou, zároveň však není vyloučeno, že určité součásti chronologicky strukturované databáze budou dále rozřazeny podle jiného klíče, v důsledku čehož takovým systémem – ve zúženém rozsahu – budou.

Naproti tomu, podle Odvolacího soudu složky vedené FSA o stížnostech žalobce neměly žádnou pravidelnou strukturu a musejí být specifikovány kontextem.

5. 3. 5. Ochrana osobních údajů třetích osob

Podle oddílu 7 (4) DPA tam, kde nemůže zpracovatel osobních údajů vyhovět žádosti o přístup k osobním údajům, aniž by musel zpřístupnit informace o jiném jednotlivci, nelze údaje poskytnout s výjimkou situace, kdy je dán souhlas této třetí osoby nebo kdy je to rozumné se zřetelem ke všem okolnostem. Nicméně, není-li žádná z těchto podmínek splněna, zpracovatel osobních údajů je povinen zpřístupnit všechny ostatní informace, kterými není odhalena totožnost jiného jednotlivce, ať již je toho dosaženo odstraněním jmen či jiných identifikátorů nebo jinak.

Žalobce namítal, že FSA upravila počítačové dokumenty tak, že z nich odstranila jména třetích osob. Odvolací soud dal najevo, že zpracovatelé osobních údajů musejí se zřetelem k čl. 7 (4) až (6) DPA zvažovat nezbytnost a proporcionalitu dříve, než přistoupí k odmítnutí žádosti o přístup k údajům. Totéž hodnotí podle čl. 7 (9) DPA soudy.

V rámci hodnocení, zda vynechání osobních údajů třetí osoby je nezbytné, Odvolací soud konstatoval, že ve skutečnosti většina úprav provedených FSA se netýkala osobních údajů žalobce. Jen ve dvou případech to mohlo být sporné. Šlo o jméno úředníka FSA, který odmítl poskytnout souhlas se sdělením vlastního jména žalobci.

K otázce proporcionality „v užším slova smyslu“ se Odvolací soud vyslovil, že nebylo záměrem zákonodárce vytvořit takový systém soudního přezkumu, který by žadatele povzbuzoval k odvolávání se úplným přezkumem, neboť by tím údajně uložil nepřiměřené břemeno na zpracovatele údajů, který ztěžka může zvažovat komponenty testu proporcionality.

5. 3. 6. Uvážení a žádost o zpřístupnění informace

Prvek uvážení předvídá čl. 7 (9) DPA a v samotné věci Durant se – vzhledem k jinak vymezenému právnímu rámci posouzení věci – přímo neuplatnil. Odvolací soud se přesto vyslovil ku prospěchu širokého uvážení, tedy s souladu s názorem zpracovatelů osobních údajů čelících požadavkům na rozsáhlé zpřístupňování údajů. Zákonná úprava však neposkytuje podklad pro odmítnutí žádosti s poukazem na složitost a náročnost vyhotovení odpovědi. Podle odůvodnění obsaženého v rozsudku ve věci Durant by měl

zpracovatel osobních údajů vyhotovení odpovědi odmítnout a poukázat na to, že žadatel vykonává své subjektivní právo coby experiment s otevřenou možností zahájení soudního sporu v návaznosti na podanou odpověď, namísto toho, aby dotaz měl skutečnou vazbu na ochranu soukromí. Za těchto okolností by podle Odvolacího soudu nebylo rozumné, aby soudy vykonávaly diskreční pravomoc podle čl. 7 (9) DPA. Zpracovatel osobních údajů by měl takovou odpověď obezřetně zvážit, ale pokud se pro ni rozhodne, uvedeného se podle judiciálního výkladu může zmocnit.

Pokud jde o test proporcionality, je třeba posuzovat vážnost zásahu, škodu jím vzniklou subjektu osobních údajů, počet postižených, náklady splnění. Článek 12 DPD požaduje po členských státech zaručit přístup k uchovávaným osobním údajům a její čl. 22 vyžaduje zajistit možnost soudního přezkumu tvrzeného porušení zaručených práv. Je tudíž sporné, zda nosné důvody rozhodnutí ve věci Durant těmto požadavkům dostojí.

6. Závěr

Z příspěvku vyplývá, že v evropských podmínkách byl ustaven sofistikovaný rámec ochrany osobních údajů, adekvátně sledující technologický vývoj. Otevřenou otázkou prozatím zůstává zejména finalizace ratifikačního procesu Lisabonské smlouvy, která prostřednictvím Charty základních práv Evropské unie nese příležitost k posílení standardů pro ochranu soukromí a osobních údajů. Vzhledem k tomu, že těžiště aplikace práva EU zůstává na soudech členských států, není bez významu, aby hledání praktických řešení tyto společně ujednané standardy příliš nerozměňovalo.

Kontaktní údaje na autora – email:

52154@mail.muni.cz