PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

01248/07/CS
WP 136

Stanovisko č. 4/2007 k pojmu osobní údaje

přijaté dne 20. června 2007

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jde o nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Jeho úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát skupiny zajišťuje ředitelství C (Civilní soudnictví, práva a občanství) Generálního ředitelství pro spravedlnost, svobodu a bezpečnost Evropské komise, B-1049 Brusel, Belgie, kancelář č. LX-46 01/43.

Internetová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1],

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

s ohledem na článek 255 Smlouvy o ES a na nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

[1] Úřední věstník L 281, 23.11.1995, s. 31; dostupná na adrese: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

I. ÚVOD

Pracovní skupina si uvědomuje potřebu provést hloubkovou analýzu pojmu osobní údaje. Z informací o současné praxi v členských státech EU vyplývá, že mezi členskými státy existuje ohledně důležitých aspektů tohoto pojmu určitá nejistota a rozdílnost v přístupech, což může v různých souvislostech nepříznivě ovlivnit řádné fungování stávajícího rámce ochrany údajů. Výsledek této analýzy jednoho z ústředních prvků z hlediska používání a výkladu pravidel ochrany údajů bude mít nutně zásadní vliv na řadu důležitých otázek. Zvláštní význam pak bude mít pro témata, jako je správa identit v rámci elektronické veřejné správy (e-Government) a elektronického zdravotnictví (e-Health), jakož i v souvislosti s identifikací na základě rádiové frekvence (RFID).

Cílem tohoto stanoviska pracovní skupiny je dosáhnout společného porozumění pojmu osobní údaje, situacím, v nichž by se měly používat vnitrostátní právní předpisy o ochraně údajů, a správnému způsobu jejich použití. Pracovat na společné definici pojmu osobní údaje znamená vymezit, co spadá a co nespadá do působnosti pravidel ochrany údajů. Dalším výsledkem této práce bude poskytnutí vodítka k tomu, jak by se měla vnitrostátní pravidla ochrany údajů používat v určitých kategoriích situací, jež se vyskytují v celé Evropě. Tím pracovní skupina zřízená podle článku 29 přispěje k jednotnému používání těchto norem, což patří k jejím hlavním úkolům.

V tomto dokumentu jsou na podporu a pro ilustraci analýzy použity příklady z vnitrostátní praxe evropských orgánů pro ochranu údajů. Většina příkladů byla upravena pouze s ohledem na vhodnost použití v tomto kontextu.

II. OBECNÉ ÚVAHY A POLITICKÉ OTÁZKY

Směrnice obsahuje široké pojetí osobních údajů.

Definice osobních údajů uvedená ve směrnici 95/46/ES (dále jen „směrnice o ochraně údajů“ nebo „směrnice“) zní takto:

„Osobními údaji (se rozumí) *veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.“*

Zde je třeba poznamenat, že tato definice odráží úmysl evropského zákonodárce směřující k širokému pojetí „osobních údajů“, který trval v průběhu celého legislativního procesu. V původním návrhu Komise je vysvětleno, že „*stejně jako v Úmluvě 108 se přijímá široká definice s cílem zahrnout veškeré informace, které mohou souviset s jednotlivcem*“[2]. V pozměněném návrhu Komise se uvádí, že „*pozměněný návrh odpovídá přání Parlamentu, aby definice „osobních údajů“ byla co nejobecnější, a tedy zahrnovala veškeré informace o identifikovatelném jednotlivci*“[3], a toto přání vzala v potaz i Rada ve svém společném postoji[4].

Cílem pravidel obsažených ve směrnici je ochrana jednotlivců.

V článku 1 směrnice 95/46/ES a článku 1 směrnice 2002/58/ES je jasně stanoven konečný účel pravidel obsažených v těchto směrnicích: ochrana základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů. To je velmi důležitý prvek, který je třeba brát v úvahu při výkladu a používání pravidel obou právních nástrojů. Podstatnou úlohu může hrát při rozhodování o tom, jak ustanovení směrnice používat v řadě situací, v nichž práva jednotlivců nejsou ohrožena, a může také varovat před jakýmkoli výkladem těchto pravidel, který by jednotlivce o ochranu jejich práv připravoval.

Z oblasti použití směrnice je vyloučena řada činností a její znění počítá s pružností umožňující vhodnou právní reakci na okolnosti, které mohou nastat.

Navzdory širokému pojetí pojmů „osobní údaje“ a „zpracování“ ve směrnici pouhá skutečnost, že lze nějakou situaci považovat za situaci zahrnující „zpracování osobních údajů“ ve smyslu příslušné definice, bez dalšího neznamená, že se na tuto situaci mají vztahovat pravidla směrnice. To je dáno především článkem 3 této směrnice. Kromě výjimek vyplývajících z působnosti práva Společenství jsou u výjimek podle článku 3 zohledněny také technický způsob zpracování (manuální neuspořádané záznamy) a záměr, pro který se údaje používají (výlučně osobní či domácí činnosti fyzické osoby). Pro určitý konkrétní případ nemusejí být použitelná všechna pravidla obsažená ve směrnici ani tehdy, jedná-li se o zpracování osobních údajů spadající do oblasti její působnosti. Řada ustanovení směrnice obsahuje značnou míru pružnosti, aby bylo dosaženo vhodné rovnováhy mezi ochranou práv subjektu údajů na jedné straně a legitimními zájmy správců údajů a třetích osob, jakož i případným veřejným zájmem, na straně druhé. Z mnoha případů takových ustanovení lze uvést například článek 6

[2] KOM(90) 314 v konečném znění, 13.9.1990, s. 19 (komentář k článku 2).
[3] KOM(92) 422 v konečném znění, 28.10.1992, s. 10 (komentář k článku 2).
[4] Společný postoj (ES) č. 1/95 přijatý Radou dne 20. února 1995, Úř. věst. C 93, 13.4.1995, s. 20.

(doba uchování údajů závisející na jejich nezbytnosti), čl. 7 písm. f) (zpracování údajů opodstatněné rovnováhou zájmů), poslední část čl. 10 písm. c) a poslední část čl. 11 odst. 1 písm. c) (informování subjektu údajů, je-li to nezbytné pro zajištění řádného zpracování) či článek 18 (výjimky z oznamovací povinnosti).

Oblast působnosti pravidel ochrany údajů by se neměla nadměrně rozšiřovat.

Nežádoucím výsledkem by bylo, kdyby se pravidla ochrany údajů používala v situacích, na které se podle původního záměru nemají vztahovat a pro které je zákonodárce nevytvořil. Způsob ochrany údajů, který chtěl zákonodárce zavést, je patrný z výše uvedených hmotněprávních výjimek podle článku 3 směrnice a z vysvětlení ve 26. a 27. bodu jejího odůvodnění.

Jedno omezení se týká způsobu zpracování údajů. V tomto ohledu je užitečné připomenout, že důvody přijetí prvních právních předpisů na ochranu údajů v sedmdesátých letech vyplývaly z toho, že nová technologie v podobě elektronického zpracování údajů umožňuje snadnější a širší přístup k osobním údajům než tradiční způsoby práce s údaji. Ochrana údajů podle směrnice je proto zaměřena na způsoby zpracování, pro něž je typické vyšší riziko „snadného přístupu k osobním údajům“ (27. bod odůvodnění). Zpracování osobních údajů neautomatizovanými postupy je do oblasti působnosti směrnice zahrnuto pouze v případě, že jsou údaje obsaženy v rejstříku nebo do něj mají být zařazeny (článek 3).

Další obecné omezení pro použití ochrany údajů podle směrnice se týká zpracování údajů za okolností, kdy o prostředcích pro identifikaci subjektu údajů neplatí, že „mohou být rozumně použity“ (26. bod odůvodnění). Touto otázkou se zabývá samostatná část tohoto stanoviska.

Je však třeba se vyvarovat také nepatřičného zužování výkladu pojmu osobní údaje.

V případech, kdy by mechanické použití každého jednotlivého ustanovení směrnice na první pohled vedlo k nadměrně zatěžujícím, či dokonce absurdním důsledkům, je třeba nejprve zkontrolovat, 1) zda situace spadá do oblasti působnosti směrnice, zvláště podle jejího článku 3 a, 2) pokud do její oblasti působnosti spadá, zda sama směrnice nebo na jejím základě přijaté vnitrostátní právní předpisy nepočítají s výjimkami nebo zjednodušeními s ohledem na zvláštní situace v zájmu dosažení vhodné právní reakce při současném zajištění ochrany práv jednotlivce a příslušných zájmů. Lepší možnost než nepatřičně zužovat výklad definice osobních údajů je uvědomit si, že při používání pravidel pro tyto údaje je k dispozici značná pružnost.

V tomto ohledu hrají zásadní úlohu vnitrostátní orgány dozoru nad ochranou údajů, a to v rámci svého úkolu sledovat používání právních předpisů o ochraně údajů, který zahrnuje podávání výkladu právních ustanovení a vydávání konkrétních pokynů pro správce a subjekty údajů. Tyto orgány by měly podporovat definici natolik širokou, aby dokázala předjímat další vývoj a aby její rozsah zahrnoval všechny „šedé zóny“, a zároveň by měly legitimně využívat pružnost, která je ve směrnici obsažena. Znění směrnice totiž vyzývá k vypracování politiky spojující široký výklad pojmu osobní údaje s vhodnou rovnováhou při používání pravidel směrnice.

III. ANALÝZA DEFINICE POJMU „OSOBNÍ ÚDAJE“ PODLE SMĚRNICE O OCHRANĚ ÚDAJŮ

Definice uvedená ve směrnici má čtyři hlavní složky, které jsou v tomto stanovisku analyzovány odděleně. Jedná se o tyto složky:

- „veškeré informace“,
- „o“ (vztah mezi informacemi a osobou),
- „identifikovaná nebo identifikovatelná“,
- (fyzická) „osoba“.

Uvedené čtyři složky jsou těsně provázány a vzájemně se podporují. Kvůli metodice použité v tomto stanovisku se však každou z nich zabýváme odděleně.

1. PRVNÍ SLOŽKA: „VEŠKERÉ INFORMACE“

Výraz „veškeré informace“ použitý ve směrnici jasně signalizuje záměr zákonodárce definovat pojem osobní údaje široce. Toto znění vyžaduje širokou interpretaci.

Z hlediska povahy informací pojem osobní údaje zahrnuje všechny druhy tvrzení o osobě. Zahrnuje tedy jak „objektivní“ informace, jako je přítomnost určité látky v krvi, tak „subjektivní“ informace, názory či hodnocení. Na druhý z uvedených typů tvrzení připadá značný podíl osobních údajů zpracovávaných například v bankovnictví pro účely posouzení spolehlivosti dlužníků („Titius je spolehlivý dlužník“), v pojišťovnictví („není pravděpodobné, že Titius brzy zemře“) nebo v souvislosti se zaměstnáním („Titius je dobrý pracovník a zaslouží si povýšení“).

Informace mohou být „osobními údaji“ bez ohledu na to, zda jsou pravdivé či prokázané. Pravidla ochrany údajů ve skutečnosti počítají s tím, že informace mohou být nesprávné, a stanovují právo subjektu údajů mít k těmto informacím přístup a napadnout je pomocí vhodných prostředků pro zajištění nápravy[5].

Z hlediska obsahu informací se pojem osobní údaje vztahuje na údaje poskytující libovolný typ informací. Patří sem samozřejmě osobní informace považované za „citlivé údaje“ podle článku 8 směrnice kvůli jejich zvláště rizikové povaze, ale i obecnější druhy informací. Výraz „osobní údaje“ označuje informace dotýkající se soukromého a rodinného života jednotlivce v úzkém smyslu, ale také informace o jakémkoli druhu činnosti, kterou se jednotlivec zabývá, například informace o jeho pracovních vztazích nebo ekonomickém či společenském chování. Zahrnuje tudíž informace o jednotlivcích bez ohledu na postavení nebo roli, v jaké daná osoba vystupuje (spotřebitel, pacient, zaměstnanec, zákazník atd.).

Příklad č. 1: profesní zvyklosti a postupy

Informace o předepisování léků (např. identifikační číslo léčivého přípravku, název léku, obsah účinné látky, výrobce, prodejní cena, informace, zda jde o první nebo opakovaný předpis na daný lék, důvody pro nasazení léku, odůvodnění zákazu nahrazení léku jiným lékem, jméno a příjmení předepisujícího lékaře, telefonní číslo atd.), ať v podobě jednotlivého předpisu nebo informací o způsobu předepisování získaných z většího počtu předpisů, lze považovat za osobní údaje o lékaři, který daný

[5] Opravu lze provést připojením opačných tvrzení nebo pomocí příslušných právních nástrojů, jako jsou mechanismy opravných prostředků.

lék předepisuje, přestože pacient je anonymní. Poskytování informací o předpisech vystavených identifikovanými nebo identifikovatelnými lékaři výrobcům léků na předpis tak představuje sdělování osobních údajů třetím osobám ve smyslu směrnice.

Tento výklad je podpořen samotným zněním směrnice. Na jedné straně je třeba vzít v úvahu, že soukromý a rodinný život je široký pojem, jak jasně stanovil Evropský soud pro lidská práva[6]. Na druhé straně jdou pravidla pro ochranu osobních údajů nad rámec ochrany uvedeného širokého pojetí práva na respektování soukromého a rodinného života. Je třeba poznamenat, že v Listině základních práv Evropské unie je ochrana osobních údajů zakotvena v článku 8 jakožto autonomní právo, které je oddělené a odlišné od práva na soukromý život uvedeného v článku 7 Listiny, a totéž platí v některých členských státech na vnitrostátní úrovni. Tomu odpovídá znění čl. 1 odst. 1 směrnice, jehož účelem je zajistit ochranu „základních práv a svobod fyzických osob, *zejména* [ale nikoli výlučně] jejich soukromí". V souladu s tím směrnice výslovně zmiňuje zpracování osobních údajů mimo rámec domácího a rodinného prostředí, například zpracování stanovené pracovněprávními předpisy (čl. 8 odst. 2 písm. b)), zpracování v souvislosti s rozsudky v trestních věcech, správními sankcemi nebo rozsudky v občanských věcech (čl. 8 odst. 5) či zpracování pro účely přímého marketingu (čl. 14 písm. b)). Tento široký přístup podpořil i Evropský soudní dvůr.[7]

Pokud jde o formát informací a nosič, který je obsahuje, zahrnuje pojem osobní údaje informace bez ohledu na formu, v jaké jsou k dispozici. Mohou mít tedy například textovou, číselnou, grafickou, fotografickou či zvukovou podobu. Patří sem mimo jiné informace na papíře stejně jako informace uložené v paměti počítače pomocí binárního kódu nebo informace na videokazetě. To logicky vyplývá ze skutečnosti, že se tento pojem vztahuje na automatické zpracování osobních údajů. Zvláště je z tohoto hlediska za osobní údaje třeba považovat zvukové a obrazové údaje, a to v míře, v jaké mohou představovat informace o jednotlivci. V tomto ohledu musí být konkrétní odkaz na údaje tvořené zvuky nebo obrazy v článku 33 směrnice chápán jako potvrzení a objasnění toho, že tento druh údajů pod uvedený pojem skutečně spadá (za předpokladu splnění všech ostatních podmínek) a že se na něj směrnice vztahuje. Jedná se o logický předpoklad ohledně ustanovení v uvedeném článku, kde je účelem posouzení otázky, zda pravidla směrnice představují vhodnou právní reakci v těchto oblastech. Tuto záležitost dále objasňuje 14. bod odůvodnění, v němž se uvádí, že „*s ohledem na význam současného rozvoje technologií pro příjem, přenos, úpravu, zaznamenání, uchování či sdělování zvukových a obrazových údajů týkajících se fyzických osob v rámci informační společnosti se tato směrnice použije i na zpracování těchto údajů*". Na druhé straně mohou být informace pokládány za osobní údaje, i když nejsou obsaženy v uspořádané databázi nebo záznamu. Jsou-li splněna další kritéria definice osobních údajů, mohou být jako osobní údaje klasifikovány rovněž informace

---

6 Rozsudek Evropského soudu pro lidská práva ve věci Amann v. Švýcarsko ze dne 16. února 2000, bod 65: „*(...) výraz „soukromý život" se nesmí vykládat restriktivně. Respektování soukromého života zahrnuje zejména právo navazovat a rozvíjet vztahy s ostatními lidmi; navíc neexistuje žádný zásadní důvod, který by ospravedlňoval vyloučení činností profesní nebo pracovní povahy z pojmu „soukromý život" (viz rozsudek ve věci Niemietz v. Německo ze dne 16. prosince 1992, řada A, č. 251-B, bod 29, s. 33–34 a výše uvedený rozsudek ve věci Halford, bod 42, s. 1015–1016). Tento široký výklad odpovídá výkladu obsaženému v Úmluvě Rady Evropy ze dne 28. ledna 1981 (...)*"

7 Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 24: „*Výraz osobní údaje použitý v čl. 3 odst. 1 směrnice 95/46 zahrnuje podle definice v čl. 2 písm. a) této směrnice veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Tento výraz nepochybně zahrnuje jméno osoby ve spojení s jejím telefonním číslem či informacemi o jejích pracovních podmínkách nebo zájmových činnostech.*"

ve volném textu elektronického dokumentu. „Osobní údaje“ tak mohou být obsaženy například ve zprávě elektronické pošty.

Příklad č. 2: telefonní bankovnictví

Jestliže je v rámci telefonního bankovnictví nahráván na pásku hlas zákazníka, který dává pokyny bance, nahrávky těchto pokynů by se měly považovat za osobní údaje.

Příklad č. 3: dohled pomocí videokamer

Obrazové záznamy jednotlivců zachycené systémem dohledu pomocí videokamer mohou být osobními údaji v té míře, do jaké je na nich tyto jednotlivce možné poznat.

Příklad č. 4: dětská kresba

Na základě neurologicko-psychiatrického vyšetření dívky, které se provede v rámci soudního řízení o tom, komu má být svěřena do péče, je předložena dívčina kresba představující její rodinu. Kresba poskytuje informace o její náladě a jejích pocitech vůči různým rodinným příslušníkům. Z toho důvodu lze výkres považovat za „osobní údaje“. Kresba skutečně podává informace o dítěti (o jeho duševním zdraví) a například také o chování jeho otce či matky. V důsledku toho mohou mít rodiče v tomto případě možnost uplatnit právo na přístup k této konkrétní informaci.

Zde je třeba se samostatně zmínit o biometrických údajích. Tyto údaje lze definovat jako biologické vlastnosti, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti. K typickým příkladům biometrických údajů patří otisky prstů, struktura sítnice, struktura obličeje či hlas, ale také geometrie ruky, struktura žil, nebo dokonce některé hluboce zakořeněné dovednosti či jiné behaviorální rysy (například vlastnoruční podpis, úhozy na klávesnici, charakteristický způsob chůze nebo řeči atd.).

Biometrické údaje jsou zvláštní tím, že je lze považovat jak za *obsah* informace o určitém jednotlivci (Titius má tyto otisky prstů), tak za prvek uvádějící nějakou informaci do *souvislosti* s tímto jednotlivcem (tohoto předmětu se dotkl někdo s těmito otisky prstů a tyto otisky prstů odpovídají Titiovým; tohoto předmětu se tudíž dotkl Titius). Z tohoto důvodu mohou fungovat jako „identifikátory“. Vzhledem k tomu, že mají jedinečnou souvislost s konkrétním jednotlivcem, mohou biometrické údaje sloužit k identifikaci tohoto jednotlivce. Uvedenou dvojí povahu mají také údaje o DNA, které podávají informace o lidském těle a umožňují jednoznačnou a jedinečnou identifikaci osoby.

Vzorky lidských tkání (například krve) jsou zdrojem, z něhož jsou biometrické údaje získávány, ale samy biometrickými údaji nejsou (podobně jako je biometrickým údajem vzor otisku prstu, avšak nikoli sám prst). Získávání informací ze vzorků tkání je proto shromažďováním osobních údajů, na které se vztahují pravidla směrnice. Shromažďování, uchovávání a využívání samotných vzorků tkání může podléhat samostatným souborům pravidel.[8]

[8] Viz doporučení Výboru ministrů Rady Evropy členským státům č. Rec (2006) 4 ze dne 15. března 2006 o výzkumu biologických materiálů lidského původu.

2. DRUHÁ SLOŽKA: „O“ (VZTAH MEZI INFORMACEMI A OSOBOU)

Tato složka definice je zásadní, protože je velmi důležité přesně zjistit, na kterých vztazích či souvislostech záleží a jak by se měly rozlišovat.

Obecně lze mít za to, že se informace nějakého jednotlivce „týkají“, pokud jsou o tomto jednotlivci.

V mnoha situacích lze tento vztah stanovit snadno. Například údaje evidované v osobním spisu v personálním oddělení se zjevně „týkají“ postavení dané osoby jakožto zaměstnance. Obdobně je to s údaji ve výsledcích lékařského testu pacienta, které jsou součástí jeho lékařských záznamů, nebo s obrazem osoby, se kterou byl natočen rozhovor na video.

Je ovšem možné uvést řadu jiných situací, u nichž nelze vždy stanovit, že se informace „týkají“ jednotlivce, se stejnou samozřejmostí jako v předchozích případech.

V některých situacích se informace, které údaje poskytují, týkají v první řadě věcí, a nikoli jednotlivců. Tyto věci obvykle někomu patří nebo mohou být určitým způsobem ovlivňovány jednotlivci nebo mít naopak vliv na jednotlivce, případně se mohou nějak nacházet ve fyzické či zeměpisné blízkosti jednotlivců nebo jiných věcí. V takovém případě je třeba mít za to, že se informace těchto jednotlivců nebo jiných věcí týkají jen nepřímo.

Příklad č. 5: hodnota domu

Hodnota konkrétního domu je informací o věci. Pokud tato informace bude sloužit pouze pro ilustraci cenové hladiny nemovitostí v nějakém okrese, pravidla ochrany údajů se nepochybně nepoužijí. Za určitých okolností by se však takové informace také měly považovat za osobní údaje. Dům je totiž majetkem svého vlastníka, a informace o něm se tudíž může použít například k vyměření nějaké daňové povinnosti této osoby. V této souvislosti by se taková informace bezpochyby měla považovat za osobní údaj.

Stejným způsobem lze analyzovat situaci, kdy se údaje týkají v první řadě procesů nebo událostí, například jedná-li se o informace o fungování stroje, který vyžaduje lidské zásahy. I zde lze mít za určitých okolností za to, že se tyto informace „týkají“ jednotlivce.

Příklad č. 6: servisní záznamy o automobilu

Servisní záznamy o automobilu, které má v držení automechanik nebo autoopravna, obsahují informace o daném vozidle, počtu ujetých kilometrů, datech servisních prohlídek, technických problémech a stavu materiálu. Tyto informace jsou v záznamech přiřazeny ke státní poznávací značce a číslu motoru, které lze uvést do souvislosti s majitelem. Jestliže autoopravna uvede vozidlo do souvislosti s majitelem pro účely fakturace, informace se budou „týkat“ majitele nebo řidiče. Je-li automobil uveden do souvislosti s automechanikem, který na něm pracoval, za účelem posouzení produktivity daného pracovníka, tyto informace se budou „týkat“ také tohoto automechanika.

Otázce, kdy lze informace pokládat za informace „týkající se“ osoby, již pracovní skupina věnovala pozornost. V rámci diskuzí o otázkách ochrany údajů souvisejících se štítky RFID pracovní skupina konstatovala, že „*údaje se týkají jednotlivce, jestliže se vztahují k totožnosti, charakteristickým znakům či chování jednotlivce nebo pokud použití těchto informací určuje nebo ovlivňuje způsob zacházení s touto osobou nebo způsob jejího hodnocení*[9]“.

Vzhledem k výše uvedeným případům by se ve stejném duchu dalo říci, že aby bylo možné údaje považovat za údaje, které se „týkají“ jednotlivce, měl by být přítomen prvek „**obsahu**“ NEBO prvek „**účelu**“ NEBO prvek „**výsledku**“.

Prvek „**obsahu**“ je přítomen v případech, kdy – v souladu s nejzjevnějším a nejběžnějším chápáním výrazu „týkat se“ ve společnosti – se informace podávají o konkrétní osobě, a to bez ohledu na jakýkoli účel, který sleduje správce údajů nebo třetí osoba, nebo na dopad těchto informací na subjekt údajů. Informace se „týkají“ nějaké osoby, jsou-li „o“ této osobě, a to je nutné posuzovat ve světle všech okolností daného případu. Výsledky lékařského rozboru se například jasně týkají pacienta a informace ve firemní složce uvedené pod jménem určitého klienta se jasně týkají tohoto klienta. Stejně tak se určité osoby týkají informace obsažené ve štítku RFID nebo čárovém kódu, který je součástí jejího dokladu totožnosti. Tak tomu bude například u budoucích cestovních pasů s čipem RFID.

Skutečnost, že se informace „týkají“ určité osoby, může vyplývat také z jejich „**účelu**“. Existenci tohoto prvku „účelu“ lze předpokládat, jestliže – při zohlednění všech okolností daného konkrétního případu – je účelem, za kterým se údaje používají nebo pravděpodobně budou používat, hodnotit jednotlivce, zacházet s ním určitým způsobem nebo ovlivnit jeho postavení či chování.

[9] Dokument pracovní skupiny č. WP 105: „Pracovní dokument o otázkách ochrany údajů souvisejících s technologií RFID“, přijatý dne 19. ledna 2005, s. 8.

Příklad č. 7: záznam hovorů z telefonu

Záznam hovorů z telefonního přístroje umístěného v kanceláři podniku poskytuje informace o hovorech provedených z tohoto telefonu, který je připojen k určité telefonní lince. Tyto informace mohou být uvedeny do souvislosti s různými subjekty. Linka byla dána k dispozici podniku a ten má také smluvní povinnost za hovory platit. V pracovní době je telefonní přístroj pod kontrolou určitého zaměstnance, který by z něj měl telefonovat. Záznam hovorů může obsahovat také informace o volaných osobách. Telefon mohou používat rovněž osoby, které mají do budovy případně přístup za nepřítomnosti daného zaměstnance (např. pracovníci úklidu). Informace o používání tohoto telefonního přístroje tak mohou být pro různé účely vztaženy k podniku, k uvedenému zaměstnanci nebo k pracovníkům úklidu (například pro kontrolu času, kdy tito pracovníci opouštějí pracoviště, protože mají povinnost telefonicky potvrzovat čas svého odchodu před zamknutím budovy). Je třeba uvést, že pojem osobní údaje se zde vztahuje jak na odchozí, tak na příchozí hovory, a to do té míry, do jaké obsahují informace o soukromém životě lidí, jejich společenských vztazích a komunikaci.

Třetí způsob, kterým se údaje mohou „týkat“ konkrétních osob, je založen na prvku „**výsledku**“. I když chybí prvek „obsahu“ a prvek „účelu“, o údajích lze mít za to, že se „týkají“ jednotlivce, jestliže – při zohlednění všech okolností daného konkrétního případu – bude mít jejich použití pravděpodobně dopad na práva a zájmy určité osoby. Přitom je třeba uvést, že není nutné, aby se u možného výsledku jednalo o velký dopad. Stačí možnost, že se v důsledku zpracování těchto údajů bude s daným jednotlivcem zacházet jinak než s ostatními osobami.

Příklad č. 8: monitorování polohy vozů taxi pro optimalizaci služeb, které má dopad na řidiče

Taxislužba zavede systém satelitního sledování, který jí umožňuje zjišťovat v reálném čase polohu volných vozů. Účelem zpracování údajů je poskytovat lepší služby a šetřit pohonné hmoty tím, že se každému zákazníkovi, který si objedná taxi, přiřadí vůz, jenž se nachází nejblíže k jeho adrese. Údaje, které takovýto systém vyžaduje, jsou přísně vzato údaji o automobilech, a nikoli o řidičích. Účelem zpracování není hodnotit výkonnost řidičů taxi, například z hlediska optimalizace jejich tras. Systém ovšem umožňuje sledovat výkonnost řidičů a kontrolovat, zda dodržují omezení rychlosti, zda používají vhodné trasy, zda jsou v daném okamžiku za volantem, nebo odpočívají mimo vůz atd. Z toho důvodu může mít značný dopad na tyto jednotlivce, a příslušné údaje tedy lze považovat za údaje, které se týkají také fyzických osob. Na jejich zpracování by se měla vztahovat pravidla ochrany údajů.

Uvedené tři prvky (obsah, účel a výsledek) je nutné chápat jako alternativní, a nikoli kumulativní podmínky. Zvláště platí, že je-li přítomen prvek obsahu, informaci lze posoudit jako informaci týkající se jednotlivce, i když zbývající prvky přítomny nejsou. Z toho nutně vyplývá, že se stejná informace může současně týkat různých jednotlivců podle toho, který prvek je přítomen ve vztahu ke každému z nich. Stejná informace se tak může týkat jednotlivce jménem Titius kvůli svému „obsahu“ (údaje jsou zjevně o Titiovi) A jednotlivce jménem Gaius kvůli svému „účelu“ (bude použita tak, aby se s Gaiem zacházelo určitým způsobem) A jednotlivce jménem Sempronius kvůli svému „výsledku“ (je pravděpodobné, že bude mít dopad na Semproniova práva a zájmy). To také znamená, že lze mít za to, že se údaje někoho týkají, i když na tohoto

člověka nejsou „zaměřeny“. Z předchozí analýzy vyplývá, že otázku, zda se údaje týkají určité osoby, je u každého jednotlivého údaje třeba zodpovědět podle jeho konkrétních vlastností. Že se informace mohou týkat různých osob je třeba mít obdobně na paměti, i při použití hmotněprávních ustanovení (např. o rozsahu práva na přístup).

Příklad č. 9: informace obsažené v zápisu ze schůze

Nutnost provádět výše uvedenou analýzu pro každou jednotlivou informaci zvlášť ilustruje příklad informací obsažených v zápisu ze schůze, kde je v souladu s obvyklým postupem zaznamenána přítomnost účastníků Titia, Gaia a Sempronia, dále výroky Titia a Gaia a konečně záznam z jednání o určitých tématech, které shrnul zapisovatel Sempronius. Za osobní údaje týkající se Titia lze pokládat pouze informace o tom, že se Titius v určitém čase a na určitém místě zúčastnil této schůze a že pronesl určité výroky. K osobním údajům týkajícím se Titia NEPATŘÍ účast Gaia na schůzi, Gaiovy výroky ani záznam z jednání o určité otázce pořízený Semproniem. Tak je tomu i v případě, že jsou tyto informace obsaženy ve stejném dokumentu a že projednání dané otázky na schůzi inicioval Titius. Na tyto informace se proto nevztahuje Titiovo právo na přístup k jeho vlastním osobním údajům. Zda a v jaké míře lze uvedené informace považovat za osobní údaje Gaia a Sempronia, bude třeba stanovit zvlášť pomocí výše popsané analýzy.

3. TŘETÍ SLOŽKA: „IDENTIFIKOVANÁ NEBO IDENTIFIKOVATELNÁ“ (FYZICKÁ OSOBA)

Směrnice vyžaduje, aby se informace týkaly fyzické osoby, která je „identifikovaná nebo identifikovatelná“, což vede k následujícím úvahám.

Obecně lze fyzickou osobu považovat za „identifikovanou“, jestliže je ve skupině osob „odlišena“ ode všech ostatních příslušníků této skupiny. V souladu s tím je fyzická osoba „identifikovatelná“, jestliže je možné ji identifikovat (přípona „-elná“ vyjadřuje možnost), ačkoli dosud identifikována nebyla. Tato druhá alternativa proto v praxi představuje prahovou podmínku určující, zda informace vyhovuje třetí složce definice.

Identifikace se obvykle provádí pomocí určitých zvláštních informací, které můžeme nazývat „identifikátory“ a které mají zvláště výsadní a těsný vztah ke konkrétnímu jednotlivci. Patří k nim vnější znaky vzhledu dané osoby, jako je výška, barva vlasů, oblečení atd., nebo vlastnosti osoby, které nejsou bezprostředně vnímatelné, jako je její povolání, funkce, jméno atd. Směrnice tyto „identifikátory“ zmiňuje v definici „osobních údajů“ v článku 2, kde je uvedeno, že fyzickou osobu „*lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity*“.

„Přímo“ či „nepřímo“ identifikovatelná

Věc je dále objasněna v komentáři k článkům pozměněného návrhu Komise, kde se uvádí, že „*osoba může být identifikována přímo jménem nebo nepřímo podle telefonního čísla, registračního čísla automobilu, čísla sociálního pojištění nebo čísla cestovního pasu nebo pomocí kombinace významných kritérií, která ji umožňuje rozeznat zúžením skupiny, do které patří (věk, povolání, bydliště atd.)*“. Ze znění tohoto tvrzení jasně vyplývá, že míra dostatečnosti určitých identifikátorů z hlediska provedení identifikace závisí na souvislostech konkrétní situace. Velmi běžné příjmení

nepostačí k identifikaci – tj. jednoznačnému určení – osoby v celé populaci země, ale pravděpodobně bude stačit k identifikaci žáka ve třídě. K identifikaci chodce ve skupině čekající u semaforu mohou stačit i vedlejší informace typu „muž v černém obleku“. Otázka, zda jednotlivec, jehož se informace týká, je, nebo není identifikovaný, tedy závisí na okolnostech daného případu.

Pokud jde o „přímo“ identifikované nebo identifikovatelné osoby, je nejběžnějším identifikátorem skutečně **jméno** a pojem „identifikovaná osoba“ v praxi nejčastěji znamená, že je známo jméno dané osoby.

Pro ověření identity je někdy jméno osoby nutné spojit s dalšími informacemi (datum narození, jména rodičů, adresa nebo fotografie obličeje), aby se zabránilo záměně této osoby za její případné jmenovce. Například informaci, že Titius dluží nějakou finanční částku, lze považovat za informaci týkající se identifikovaného jednotlivce, protože je spojena se jménem osoby. Jméno je informace, která ukazuje, že daný jednotlivec používá danou kombinaci písmen a zvuků, aby se odlišil a aby ho mohly odlišit ostatní osoby, s nimiž navazuje vztahy. Jméno může být také východiskem vedoucím k informacím o tom, kde dotyčná osoba bydlí nebo kde je k zastižení, a může být zdrojem informací o rodinných příslušnících (prostřednictvím příjmení) a o řadě různých právních a společenských vztahů s tímto jménem spojených (záznamy o vzdělání, lékařské záznamy, bankovní účty). Pokud je se jménem spojeno vyobrazení, může být dokonce možné dozvědět se o vzhledu dané osoby. Všechny tyto nové informace spojené se jménem mohou někomu dovolit, aby „zaostřil“ na konkrétního člověka, a původní informace je tak pomocí identifikátorů spojena s fyzickou osobou, kterou lze odlišit od jiných osob.

Co se týče „nepřímo“ identifikovaných nebo identifikovatelných osob, tato kategorie se obvykle vztahuje k jevu „jedinečných kombinací“, ať malého či velkého rozsahu. I v případech, kdy rozsah dostupných identifikátorů *prima facie* nikomu neumožňuje jednoznačně určit konkrétní osobu, může být tato osoba přesto „identifikovatelná“, protože ve spojení s dalšími informacemi (které může, ale nemusí mít v držení správce údajů) tyto informace umožní odlišení daného jednotlivce od jiných osob. Právě zde se uplatní směrnice se svým odkazem na „jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“. Některé charakteristiky jsou natolik jedinečné, že lze danou osobu identifikovat velmi snadno („současný předseda vlády Španělska“), ale za určitých okolností může být dosti směrodatná i kombinace údajů v rovině kategorií (věková kategorie, regionální původ atd.), zvláště pokud existuje přístup k nějakému druhu doplňkových informací. Tento jev důkladně prostudovali statistici, kteří vždy věnují velkou pozornost prevenci porušení důvěrnosti.

Příklad č. 10: útržkovité informace v tisku

Jsou zveřejněny informace o případu trestné činnosti z minulosti, který si ve své době získal velkou pozornost veřejnosti. V současném zveřejnění není uveden žádný z tradičních identifikátorů, především žádná jména či data narození zúčastněných osob.

Zdá se však, že není nepřiměřeně obtížné získat dodatečné informace, které by umožnily zjistit totožnost hlavních aktérů – např. vyhledáním novin z příslušného období. Lze skutečně předpokládat, že není zcela nepravděpodobné, že někdo podnikne kroky (jako je vyhledání starých novin), kterými s největší pravděpodobností získá jména a další identifikátory osob, jichž se případ týká. Zdá se tedy, že informace v tomto příkladu je možné opodstatněně považovat za „informace o identifikovatelných osobách", a tedy za „osobní údaje".

Zde je třeba poznamenat, že i když je identifikace pomocí jména v praxi nejběžnější, jméno nemusí být nutné pro identifikaci jednotlivce ve všech případech. Tak tomu může být, jsou-li k jednoznačnému určení osoby použity jiné „identifikátory". Například počítačové záznamy evidující osobní údaje evidovaným osobám obvykle přiřazují jedinečné identifikátory, aby nemohlo dojít k záměně dvou osob v záznamech. Také na internetu je díky nástrojům pro sledování internetového provozu snadné identifikovat chování určitého počítače, a tedy i jeho uživatele. Z různých prvků se tak složí osobnost jednotlivce, aby jí mohla být připisována určitá rozhodnutí. I bez jakýchkoli dotazů na jméno a adresu daného jednotlivce je možné tuto osobu zařadit na základě socioekonomických, psychologických, filozofických a dalších kritérií a připisovat jí určitá rozhodnutí, protože kontaktní bod (počítač), který používá, již nezbytně nevyžaduje odhalení její identity v úzkém slova smyslu. Jinými slovy možnost identifikovat jednotlivce již nutně neznamená schopnost zjistit jeho jméno a definice osobních údajů tuto skutečnost odráží[10].

Evropský soudní dvůr se v tomto smyslu vyjádřil, když konstatoval, že „*uvádění různých osob na internetové stránce a jejich identifikace jménem nebo jinými prostředky, například uvedením jejich telefonních čísel nebo informací o jejich pracovních podmínkách a zájmových činnostech, představuje zpracování osobních údajů (...) ve smyslu (...) směrnice 95/46/ES*"[11].

Příklad č. 11: žadatelé o azyl

Žadatelům o azyl, kteří skrývají svá skutečná jména, byly v azylovém zařízení přiděleny číselné kódy pro správní účely. Tato čísla budou sloužit jako identifikátory, takže ke každému z nich budou připojovány různé informace o pobytu daného žadatele o azyl v tomto zařízení. Ve spojení s fotografií nebo jinými biometrickými ukazateli bude mít číselný kód těsný a bezprostřední vztah k fyzické osobě, kterou tak bude možné odlišit od ostatních žadatelů o azyl a přiřazovat k ní různé informace. Tyto informace se pak budou týkat „identifikované" fyzické osoby.

[10] Zpráva o použití zásad ochrany údajů v případě celosvětových telekomunikačních sítí, T-PD (2004) 04 v konečném znění, kterou vypracoval Yves Poullet a kolektiv pro výbor T-PD Rady Evropy, bod 2.3.1.

[11] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 27.

V čl. 8 odst. 7 je také stanoveno, že „členské státy určí podmínky, za kterých může být předmětem zpracování vnitrostátní identifikační číslo nebo jakýkoli jiný identifikátor obecného významu“. Je důležité uvědomit si smysl tohoto ustanovení, které neobsahuje žádnou konkrétní zmínku o tom, jaký druh podmínek by měly členské státy zvolit, ale přesto je součástí článku, který se týká citlivých údajů. V 33. bodu odůvodnění je tento druh údajů popsán jako „*údaje, které svou povahou mohou porušit základní svobody nebo soukromí*“. Je možné se rozumně domnívat, že zákonodárce mohl mít s ohledem na vnitrostátní identifikační čísla obdobné obavy vzhledem k tomu, jak výrazný potenciál tato čísla mají pro snadné a jednoznačné propojení různých informací o daném jednotlivci.

Prostředky identifikace

Zvláštní pozornost výrazu „identifikovatelný“ je věnována ve 26. bodu odůvodnění směrnice, kde je uvedeno, že „*pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou pro identifikaci dané osoby*“. To znamená, že pouhá hypotetická možnost jednoznačného určení nějaké osoby nepostačuje k tomu, aby tato osoba byla považována za „identifikovatelnou“. Jestliže s přihlédnutím ke „*všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou*“, taková možnost neexistuje nebo je zanedbatelná, daná osoba by se neměla považovat za „identifikovatelnou“ a informace o ní za „osobní údaje“. Při uplatňování kritéria přihlédnutí ke „*všem prostředkům, které mohou být rozumně použity jak správcem tak jakoukoli jinou osobou*“ je třeba zvláště dbát na zohlednění všech faktorů, které v daném případě hrají roli. Jedním, avšak ne jediným faktorem jsou náklady na provedení identifikace. Kromě nich by měly být vzaty v potaz zamýšlený účel zpracování a jeho struktura, výhody očekávané správcem údajů, zájmy jednotlivců, které jsou v sázce, i riziko organizačních selhání (např. porušení povinnosti zachovávat důvěrnost) a technických problémů. Na druhé straně se jedná o dynamické kritérium, při jehož použití by měly být zohledněny aktuální stav technologií v době zpracování údajů a možnosti jejich vývoje za dobu, po kterou bude zpracování trvat. Je možné, že s prostředky, které mohou být rozumně použity v současnosti, nelze identifikaci provést. Je-li zamýšlená doba uchování údajů jeden měsíc, lze předpokládat, že identifikace nebude možná po dobu existence daných informací, které by se proto neměly považovat za osobní údaje. Pokud se však plánuje údaje uchovávat 10 let, správce by měl vzít v úvahu, že identifikace může být proveditelná například v devátém roce jejich existence, kdy by se z nich v důsledku toho mohly stát osobní údaje. Systém by měl být navržen tak, aby se dokázal přizpůsobovat takovým změnám v okamžiku, kdy nastanou, a aby do něj bylo možné včas začleňovat vhodná technická a organizační opatření.

Příklad č. 12: zveřejnění rentgenových snímků spolu s rodným jménem pacienta

Ve vědeckém časopise byl zveřejněn rentgenový snímek pacientky spolu s jejím rodným jménem, které je velice neobvyklé. Uvedení rodného jména této osoby ve spojení s tím, že její příbuzní nebo známí věděli, že trpí určitou chorobou, ji učinilo identifikovatelnou pro řadu lidí. V takovém případě by se rentgenový snímek považoval za osobní údaj.

Příklad č. 13: údaje z farmaceutického výzkumu

Nemocnice nebo jednotliví lékaři předávají údaje z lékařských záznamů svých pacientů určité společnosti pro účely lékařského výzkumu. Při tom se nepoužívají jména

pacientů, nýbrž pouze sériová čísla, která se náhodně přiřazují jednotlivým klinickým případům, aby se zajistila konzistence a zabránilo se záměně s informacemi o jiných pacientech. Jména pacientů zůstávají výlučně v držení příslušných lékařů, kteří jsou vázáni lékařským tajemstvím. Údaje neobsahují žádné dodatečné informace, které by v kombinaci s těmito údaji umožňovaly identifikaci pacientů. Kromě toho byla přijata všechna další potřebná opatření, ať již právní, technické nebo organizační povahy, pro prevenci identifikace a identifikovatelnosti subjektů údajů. Za těchto okolností může orgán pro ochranu údajů usoudit, že v rámci zpracování údajů prováděného farmaceutickou společností neexistují žádné prostředky, které by mohly být rozumně použity k identifikaci subjektů údajů.

Jak je uvedeno výše, při posuzování „*všech prostředků, které mohou být rozumně použity*“ pro identifikaci osob, bude k významným faktorům patřit účel, který správce údajů zpracováním sleduje. Vnitrostátní orgány pro ochranu údajů se setkaly s případy, kdy správce údajů tvrdil, že se zpracovávají pouze rozptýlené informace neobsahující odkaz na jméno ani jiné přímé identifikátory, a prosazoval, aby se tyto údaje nepovažovaly za osobní údaje a aby se na ně nevztahovala pravidla ochrany údajů. Na druhé straně ovšem zpracování těchto informací mělo smysl pouze za předpokladu, že umožňovalo identifikaci konkrétních jednotlivců a určitý způsob zacházení s nimi. V takovýchto případech, kdy identifikace jednotlivců vyplývá z účelu zpracování, lze předpokládat, že správce údajů nebo jakákoli jiná zúčastněná osoba má nebo bude mít prostředky, „které mohou být rozumně použity“ k identifikaci subjektu údajů. Tvrzení, že jednotlivci nejsou identifikovatelní v situaci, kdy je účelem zpracování právě jejich identifikace, by obsahovalo jasný vnitřní rozpor. Proto je zde třeba mít za to, že se informace týkají identifikovatelných jednotlivců, a na jejich zpracování by se měla vztahovat pravidla ochrany údajů.

Příklad č. 14: dohled pomocí videokamer

Výše uvedené má zvláštní význam v souvislosti s dohledem pomocí videokamer, kdy správci údajů často tvrdí, že k identifikaci dojde jen u malé části shromážděného materiálu, a že tedy žádné osobní údaje nejsou zpracovávány, dokud identifikace v těchto několika málo případech skutečně neproběhne. Účelem dohledu pomocí videokamer však je právě identifikace osob zachycených na záznamu ve všech případech, kdy to správce pokládá za nezbytné. Celý systém jako takový se proto musí považovat za zpracovávání údajů o identifikovatelných osobách, i když některé natočené osoby v praxi identifikovatelné nejsou.

Příklad č. 15: dynamické IP adresy

Pracovní skupina již uvedla, že IP adresy považuje za údaje týkající se identifikovatelné osoby. Konstatovala totiž, že „*poskytovatelé přístupu k internetu a správci sítí LAN mohou s použitím přiměřených prostředků identifikovat uživatele internetu, kterým přiřadili IP adresy, protože obvykle soustavně „protokolují“ do souboru datum, čas a trvání připojení a dynamickou IP adresu přidělenou uživateli. Totéž platí o poskytovatelích internetových služeb, kteří mají protokol na HTTP serveru. V těchto případech lze nepochybně hovořit o osobních údajích ve smyslu čl. 2 písm. a) směrnice ...)*“[12]

[12] Dokument č. WP 37: Soukromí na internetu – integrovaný přístup EU k ochraně údajů na internetu, přijatý dne 21. listopadu 2000.

Zejména v případech, kdy se zpracování IP adres provádí za účelem identifikace uživatelů počítače (například ze strany majitelů autorských práv, kteří chtějí stíhat uživatele počítačů za porušování práv duševního vlastnictví), správce údajů předjímá, že „prostředky, které mohou být rozumně použity“ k identifikaci těchto osob budou k dispozici, např. prostřednictvím soudů, na něž se obrátí, (jinak by sběr informací neměl smysl), a tyto informace by se proto měly považovat za osobní údaje.

Zvláštním případem by byl nějaký druh IP adres, které za určitých okolností z různých technických a organizačních důvodů skutečně neumožňují identifikaci uživatele. Příkladem mohou být IP adresy přidělované počítači v internetové kavárně, kde se nevyžaduje prokázání totožnosti zákazníků. Zde by se dalo tvrdit, že údaje o používání počítače X shromážděné za určité časové období neumožňují identifikaci uživatele s použitím rozumných prostředků, a tedy nejsou osobními údaji. Je ovšem třeba poznamenat, že poskytovatelé internetových služeb s největší pravděpodobností nebudou vědět, zda daná IP adresa umožňuje, nebo neumožňuje identifikaci, a že údaje spojené s touto adresou budou zpracovávat stejným způsobem jako informace spojené s IP adresami řádně zaregistrovaných uživatelů, kteří jsou identifikovatelní. Pokud tedy poskytovatel internetových služeb není schopen s naprostou jistotou odlišit údaje odpovídající uživatelům, kteří nemohou být identifikováni, bude muset pro jistotu nakládat se všemi informace o IP adresách jako s osobními údaji.

Příklad č. 16: škody, které způsobuje graffiti

Vozy pro přepravu cestujících, které vlastní určitá dopravní společnost, jsou opakovaně poškozovány graffiti. Za účelem stanovení výše škody a pro snazší uplatnění právních nároků vůči tvůrcům graffiti vytvoří tato společnost rejstřík, který obsahuje informace o okolnostech vzniku škody a vyobrazení poškozených věcí i „tagů“ neboli „podpisů“ těchto tvůrců. V okamžiku vložení informací do rejstříku jsou původci škody neznámí a neví se ani, komu patří který „podpis“. Může se stát, že se to nezjistí nikdy. Účelem zpracování je však právě identifikovat jednotlivce, kterých se informace týkají, jakožto původce škody, aby vůči nim bylo možné vznést právní nároky. Takové zpracování má smysl, jestliže správce údajů považuje za rozumně pravděpodobné, že prostředky k identifikaci těchto jednotlivců jednou budou existovat. Informace na vyobrazení by se měly pokládat za informace týkající se „identifikovatelných“ jednotlivců a informace v rejstříku za „osobní údaje“ a na jejich zpracování by se měla vztahovat pravidla ochrany údajů, která takové zpracování za určitých okolností umožňují jakožto legitimní, jsou-li přijata určitá ochranná opatření.

Jestliže identifikace subjektu údajů není součástí účelu zpracování, hrají důležitou úlohu technická opatření, která mají identifikaci zabránit. Zavedení vhodných nejmodernějších technických a organizačních opatření na ochranu údajů před identifikací může rozhodnout o tom, že se osoby nebudou považovat za identifikovatelné s přihlédnutím ke *všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou k* identifikaci jednotlivců. V tomto případě zavedení takových opatření není *důsledkem* právní povinnosti vyplývající z článku 17 směrnice (který se použije, pouze pokud informace jsou osobními údaji), nýbrž *podmínkou* toho, aby informace za osobní údaje právě považovány nebyly a aby jejich zpracování nespadalo do oblasti působnosti směrnice.

Pseudonymizované údaje

Pseudonymizace je proces skrytí identit, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. To má zvláštní význam v oblasti výzkumu a statistiky.

Pseudonymizaci lze provést pomocí korespondenčních tabulek identit a k nim příslušejících pseudonymů nebo pomocí obousměrných kryptografických algoritmů pro pseudonymizaci. V takovém případě je možné identity zpětně vysledovat. Identity lze skrýt také způsobem, který jakoukoli zpětnou identifikaci znemožňuje, např. pomocí jednosměrné kryptografie, která obecně generuje anonymizované údaje.

Efektivnost postupu pseudonymizace závisí na řadě faktorů (na tom, v jaké fázi se použije a nakolik je zabezpečen před zpětným vysledováním identit; na velikosti souboru, jehož je jednotlivec součástí; na možnosti spojit jednotlivé operace nebo záznamy se stejnou osobou atd.). Pseudonymy by měly být náhodné a nepředvídatelné. Počet možných pseudonymů by měl být natolik velký, aby stejný pseudonym nikdy nebyl náhodně vybrán dvakrát. Vyžaduje-li se vysoká úroveň zabezpečení, musí se množina možných pseudonymů alespoň rovnat rozpětí hodnot bezpečných kryptografických hash funkcí.[13]

Pseudonymizované údaje, jež umožňují zpětné vysledování, lze pokládat za informace o jednotlivcích, které jsou *nepřímo identifikovatelné*. Použití pseudonymu skutečně znamená, že jednotlivce je možné zpětně dohledat, takže lze zjistit jeho identitu – ovšem pouze za předem stanovených podmínek. V tomto případě se pravidla ochrany údajů sice použijí, ale rizika pro jednotlivce, která jsou spojena se zpracováním takovýchto nepřímo identifikovatelných informací, budou nejčastěji nízká, takže tato pravidla bude možné oprávněně použít pružněji, než kdyby byly zpracovávány informace o přímo identifikovatelných jednotlivcích.

Údaje kódované pomocí klíče

Údaje kódované pomocí klíče jsou klasickým příkladem pseudonymizace. Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně.

Příklad č. 17: neagregované údaje pro statistické účely

Při posuzování toho, zda prostředky k identifikaci „mohou být rozumně“ použity, je důležité brát v potaz všechny okolnosti. To lze ilustrovat na příkladu osobních informací zpracovávaných vnitrostátním statistickým úřadem, které se v určité fázi uchovávají v neagregované podobě a týkají se konkrétních jednotlivců. Tito jednotlivci však nejsou označeni jménem, nýbrž kódem (např. osoba s kódem X1234 vypije sklenici vína častěji než třikrát za týden). Klíč k těmto kódům (tabulku přiřazující kódy ke jménům osob) statistický úřad uchovává odděleně. Lze mít za to, že tento klíč „může být rozumně použit“ statistickým úřadem, a soubor informací týkajících se jednotlivců proto může být považován za osobní údaje, a úřad by s ním měl nakládat podle pravidel ochrany údajů. Následně je možné si představit, že se seznam s údaji o zvyklostech spotřebitelů ohledně pití vína předá národní organizaci výrobců vína,

[13] Viz pracovní dokument „Technologie zlepšující ochranu soukromí“ pracovní skupiny pro „technologie zlepšující ochranu soukromí“ výboru pro „technické a organizační aspekty ochrany údajů“ německých spolkových a zemských komisařů pro ochranu údajů (říjen 1997); zveřejněný na adrese: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm.

která chce tyto statistické údaje využít na podporu svého veřejného stanoviska. Má-li se určit, zda tento seznam informací stále představuje osobní údaje, mělo by se posoudit, zda „*s přihlédnutím ke všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*“, mohou být jednotliví spotřebitelé vína identifikováni.

Je-li pro každou konkrétní osobu použit jedinečný kód, riziko identifikace nastává, kdykoli lze získat přístup k šifrovacímu klíči. Při rozhodování o tom, zda mohou být s *přihlédnutím ke všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*, příslušné osoby identifikovány, *a* tedy zda je tyto informace třeba považovat za „osobní údaje“, je proto nutné vzít v potaz faktory, jako jsou riziko počítačového průniku zvenčí, pravděpodobnost, že někdo z odesílající organizace poruší profesní tajemství a klíč poskytne, a proveditelnost nepřímé identifikace. Pokud informace osobními údaji jsou, použijí se pravidla ochrany údajů. Jiná otázka je, že při uplatnění těchto pravidel by bylo možné zohlednit, zda byla rizika pro jednotlivce snížena, a stanovit pro zpracování přísnější nebo mírnější podmínky s využitím pružnosti, kterou pravidla směrnice umožňují.

Jestliže kódy naopak jedinečné nejsou a stejný číselný kód (např. „123“) je použit pro označení jednotlivců v různých městech a pro údaje z různých let (konkrétní jednotlivec je odlišen pouze v rámci daného roku a v rámci vzorku ze stejného města), mohl by správce nebo třetí osoba konkrétního jednotlivce identifikovat pouze v případě, že by věděl, kterého roku a kterého města se ten který údaj týká. Pokud byly tyto doplňující informace odstraněny a pomocí rozumných prostředků je nelze získat zpět, bylo by možné mít za to, že se informace netýkají identifikovatelných jednotlivců, a pravidla ochrany údajů by se na ně nevztahovala.

Tento druh údajů se běžně používá při klinických zkouškách léčivých přípravků. Právní rámec pro provádění těchto činností stanoví směrnice 2001/20 ze dne 4. dubna 2001 o uplatňování správné klinické praxe při provádění klinických hodnocení[14]. Lékař / výzkumný pracovník („zkoušející“), který lék testuje, shromažďuje informace o klinických výsledcích u jednotlivých pacientů, které označí kódy. Farmaceutické společnosti nebo jiným zúčastněným stranám („zadavatelům“) výzkumný pracovník tyto informace předává pouze v této kódované podobě, protože je zajímají pouze biostatistické informace. Zkoušející ovšem odděleně uchovává klíč, který kódy přiřazuje k běžným informacím umožňujícím oddělenou identifikaci pacientů. Zkoušející je povinen tento klíč uchovávat v zájmu ochrany zdraví pacientů pro případ, že se v souvislosti s lékem projeví nějaká nebezpečí. Jde o to, aby v případě potřeby mohli být jednotliví pacienti identifikováni a náležitě léčeni.

Zde vzniká otázka, zda lze údaje používané pro klinické zkoušky pokládat za údaje týkající se „identifikovatelných“ fyzických osob, čili za údaje, na které se vztahují pravidla ochrany údajů. V souladu s již popsanou analýzou je pro určení, zda je osoba identifikovatelná, třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. V tomto případě je identifikace jednotlivců (kvůli nasazení vhodné léčby v případě potřeby) jedním z účelů zpracování údajů kódovaných pomocí klíče. Farmaceutická společnost nastavila prostředky pro zpracování údajů, včetně organizačních opatření a svých vztahů s výzkumným pracovníkem, který má v držení klíč, takovým způsobem, že identifikace jednotlivců nejen *může* nastat, ale za určitých okolností nastat *musí*.

[14] Úř. věst. L 121, 1.5.2001, s. 34.

Identifikace pacientů je tak nedílnou součástí účelů a prostředků zpracování. V takovém případě lze učinit závěr, že tyto údaje kódované pomocí klíče představují informace týkající se identifikovatelných fyzických osob pro všechny strany, které se mohou podílet na případné identifikaci, a měla by se na ně vztahovat pravidla uvedená v právních předpisech o ochraně údajů. To ovšem neznamená, že i každý další správce údajů zpracovávající stejný soubor kódovaných údajů bude zpracovávat osobní údaje, pokud je v konkrétním režimu, v němž tito jiní správci působí, zpětná identifikace explicitně vyloučena a v tomto směru byla přijata vhodná technická opatření.

V jiných oblastech výzkumu nebo jiných částech stejného projektu mohla být zpětná identifikace subjektu údajů vyloučena při přípravě protokolů a postupů, a to například z důvodu, že v nich nejsou přítomny žádné léčebné aspekty. Z technických nebo jiných důvodů může přesto existovat způsob, jak zjistit, kterým osobám odpovídají které klinické údaje. Nepředpokládá se však a ani se neočekává, že by tato identifikace za jakýchkoli okolností proběhla, a byla zavedena vhodná technická opatření (např. kryptografická, nevratné zašifrování pomocí hash algoritmu), která identifikaci brání. I když k identifikaci některých subjektů údajů může dojít navzdory všem těmto protokolům a opatřením (vinou nepředvídatelných okolností, jako je náhodná shoda vlastností subjektu údajů, které odhalí jeho identitu), v tomto případě se s přihlédnutím ke *všem prostředkům, které mohou být rozumně použity správcem nebo jakoukoli jinou osobou*, informace zpracovávané původním správcem nemusejí považovat za informace týkající se identifikovaných nebo identifikovatelných jednotlivců. Na jejich zpracování se tak nemusejí vztahovat ustanovení směrnice. Avšak v případě nového správce, který fakticky získal přístup k identifikovatelným informacím, se tyto informace nepochybně budou považovat za „osobní údaje“.

Často kladená otázka (FAQ) 14 bod 7 zásad bezpečného přístavu

Otázka údajů kódovaných pomocí klíče ve farmaceutickém výzkumu je řešena v rámci zásad bezpečného přístavu[15]. FAQ 14 bod 7 zní takto:

FAQ 14 – Léčiva

7. Ot.: Údaje určené pro výzkum jsou u zdroje zásadně kódovány pomocí unikátního klíče vedoucím výzkumným pracovníkem tak, aby nebyla zřejmá totožnost konkrétních subjektů údajů. Farmaceutické společnosti financující takový výzkum klíč neobdrží. Kód k unikátnímu klíči má pouze výzkumný pracovník, který tak může za určitých okolností danou osobu identifikovat (např. je-li potřebný následný lékařský dohled). Představuje předání takto kódovaných údajů z EU do Spojených států předání osobních údajů, které podléhá zásadám „bezpečného přístavu“?

7. Odp.: Ne. V tomto případě nejde o předání osobních údajů, které by podléhalo zásadám „bezpečného přístavu“.

Pracovní skupina soudí, že toto tvrzení v zásadách bezpečného přístavu není neslučitelné s výše uvedenou argumentací ve prospěch toho, aby se takové informace pokládaly za osobní údaje, na které se vztahuje směrnice. Tato FAQ ve skutečnosti není dostatečně přesná, protože neuvádí, komu a za jakých podmínek se údaje předávají. Pracovní skupina rozumí této FAQ tak, že se týká případů, kdy jsou údaje kódované pomocí klíče odesílány příjemci v USA (například farmaceutické

[15] Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000, Úř. věst. L 215/7, 25.8.2000.

společnosti), který obdrží pouze údaje kódované pomocí klíče a nikdy nebude znát totožnost pacientů. Ta je a v případě potřeby léčby bude známa pouze lékaři / výzkumnému pracovníkovi v EU, nikdy však společnosti v USA.

Anonymní údaje

„Anonymní údaje“ ve smyslu směrnice lze definovat jako jakékoli informace týkající se fyzické osoby, z nichž tato osoba nemůže být identifikována ani správcem ani jakoukoli jinou osobou s *přihlédnutím ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou* pro identifikaci daného jednotlivce. „Anonymizovanými údaji“ se proto rozumí anonymní údaje, které dříve odkazovaly na identifikovatelnou osobu, ale u nichž tuto identifikaci již nelze provést. Na tento pojem odkazuje také 26. bod odůvodnění, když říká, že „*zásady ochrany se nevztahují na údaje, které byly anonymizovány tak, že subjekt údajů již není identifikovatelný*“. I zde posouzení otázky, zda údaje umožňují identifikaci jednotlivce a zda informace lze, nebo nelze považovat za anonymní, závisí na okolnostech a analýzu je třeba provádět případ od případu se zvláštním ohledem na míru, v jaké mohou být rozumně použity prostředky pro identifikaci, jak je popsáno ve 26. bodu odůvodnění. Toto má zvláštní význam v případech statistických informací, které sice mohou být prezentovány v podobě agregovaných údajů, ale původní vzorek není dostatečně velký a další informace mohou umožnit identifikaci jednotlivců.

Příklad č. 18: statistická šetření a spojení rozptýlených informací

Kromě obecné povinnosti dodržovat pravidla ochrany údajů mají statistici v zájmu zajištění anonymity statistických šetření také zvláštní povinnost zachovávat profesní tajemství. Tato pravidla jim zakazují zveřejňovat neanonymní údaje. Musejí tedy zveřejňovat agregované statistické údaje, jež v žádném případě nelze přiřadit k identifikované osobě, která je předmětem statistiky. Toto pravidlo je zvláště významné v souvislosti se zveřejňováním výsledků sčítání lidu. V každé situaci by měl být stanoven práh, při jehož nedosažení se má za to, že dotčené osoby lze identifikovat. Jestliže se zdá, že nějaké kritérium vede k identifikaci v dané kategorii osob, pak by bez ohledu na velikost této kategorie (např. když ve městě s 6 000 obyvateli působí jen jeden lékař) mělo být toto „diskriminační“ kritérium zcela vypuštěno nebo by měla být doplněna další kritéria, aby došlo k „rozředění“ výsledků o dané osobě, a tak bylo možné zachovat statistické tajemství.

Příklad č. 19: zveřejnění snímků z dohledu pomocí videokamer

Majitel prodejny ve svém obchodě nainstaluje systém dohledu pomocí videokamer. Následně v obchodě zveřejní snímky zlodějů, kteří byli díky tomuto systému zadrženi. Po zásahu policie obličeje zlodějů začerní. Avšak i po této úpravě existuje možnost, že osoby na fotografiích poznají jejich přátelé, příbuzní nebo sousedé, například proto, že se stále dají rozeznat jejich postavy, účesy a oblečení.

4. ČTVRTÁ SLOŽKA: (FYZICKÁ) „OSOBA“

Ochrana, kterou poskytují pravidla směrnice, se vztahuje na fyzické osoby, tj. na lidi. V tomto smyslu je právo na ochranu osobních údajů univerzálním právem, které není omezeno na státní příslušníky či obyvatele určité země. To je výslovně uvedeno v 2. bodu odůvodnění směrnice, kde se konstatuje, že „*systémy zpracování údajů slouží*

lidem“ a že „*musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob*“.

Na pojem fyzická osoba odkazuje článek 6 Všeobecné deklarace lidských práv, který zní: „*Každý má právo na to, aby byla všude uznávána jeho právní osobnost*.“ Pojem právní osobnosti (právní subjektivity) lidí, kterou se rozumí způsobilost být subjektem právních vztahů a která začíná narozením a končí smrtí, přesněji vymezují právní předpisy členských států, obvykle v oblasti občanského práva. Osobními údaji jsou proto v zásadě údaje týkající se identifikovaných nebo identifikovatelných *žijících jednotlivců*. Z toho pro účely této analýzy vyplývá řada otázek.

Údaje o zemřelých osobách

Informace, které se týkají zemřelých jednotlivců, by se proto v zásadě neměly pokládat za osobní údaje, na které se vztahují pravidla směrnice, protože zemřelí již nejsou fyzickými osobami podle občanského práva. V některých případech se však údajům o zemřelých přesto může nepřímo dostat určité ochrany.

Zaprvé nemusí být správce údajů schopen zjistit, zda osoba, které se údaje týkají, je stále naživu, nebo již zemřela. Ale i v případě, že to zjistit dokáže, mohou být informace o zemřelých bez rozlišení zpracovávány ve stejném režimu jako informace o žijících osobách. Vzhledem k údajům o žijících jednotlivcích se na správce údajů vztahují povinnosti v oblasti ochrany údajů uložené směrnicí, a v praxi pro něj proto bude pravděpodobně jednodušší zpracovávat i údaje o zemřelých způsobem, který ukládají pravidla ochrany údajů, než oba soubory údajů oddělovat.

Zadruhé mohou informace o zemřelých jednotlivcích odkazovat také na žijící osoby. Například z informace, že zemřelá Gaia trpěla hemofilií, vyplývá, že jí trpí i její syn Titius, protože toto onemocnění souvisí s genem v chromozomu X. Jestliže tedy informace, které jsou údaji o zemřelých, lze současně považovat za informace týkající se také žijících osob a za osobní údaje, na které se vztahuje směrnice, mohou osobní údaje zemřelých nepřímo požívat ochrany podle pravidel ochrany údajů.

Zatřetí mohou být informace o zemřelých osobách předmětem zvláštní ochrany, kterou poskytují jiné soubory pravidel než právní předpisy o ochraně údajů. Tato pravidla vymezují hranice toho, co se někdy označuje jako „*personalitas praeterita*“. Povinnost zdravotníků zachovávat důvěrnost nekončí smrtí pacienta. Vnitrostátní právní předpisy o právu na ochranu osobní pověsti a cti mohou poskytovat ochranu také památce zemřelých.

Začtvrté, jak připomněl ESD[16], nic nebrání členskému státu, aby oblast působnosti vnitrostátních právních předpisů, kterými se provádí směrnice 95/46/ES, rozšířil na oblasti nezahrnuté do působnosti této směrnice za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství. Je možné, že se vnitrostátní zákonodárce v některých státech rozhodne rozšířit ustanovení vnitrostátních právních

[16] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 98.

předpisů o ochraně údajů i na některé aspekty zpracování údajů o zemřelých osobách, pokud to bude opodstatněno legitimním zájmem.[17]

Nenarozené děti

Míra, v jaké se pravidla ochrany údajů mohou použít před narozením, závisí na obecném postoji vnitrostátních právních systémů k ochraně nenarozených dětí. Především s ohledem na dědická práva některé členské státy uznávají zásadu, že počaté, ale dosud nenarozené děti se pokládají za narozené, pokud jde o jejich prospěch (a tak mohou dědit či přijímat dary), za podmínky, že se skutečně narodí. V jiných členských státech poskytují konkrétní ochranu zvláštní právní předpisy, a to za stejné podmínky. Aby bylo možné určit, zda vnitrostátní předpisy o ochraně údajů chrání také informace o nenarozených dětech, je třeba posoudit tento obecný přístup vnitrostátního právního systému spolu s účelem pravidel ochrany údajů, kterým je ochrana jednotlivce.

Další otázka souvisí s úvahou, že obecná reakce právního systému vychází z předpokladu, že situace nenarozených dětí je časově omezena na dobu těhotenství, a nebere se v úvahu, že ve skutečnosti může trvat podstatně déle – jako v případě zmrazených embryí. Konkrétní právní reakce mohou být součástí zvláštních předpisů o metodách reprodukce, které se zabývají použitím lékařských nebo genetických informací o embryích.

Právnické osoby

Jelikož v definici osobních údajů se odkazuje na jednotlivce, tj. fyzické osoby, na informace týkající se právnických osob se směrnice v zásadě nevztahuje, a ochrana poskytovaná směrnicí se v jejich případě nepoužije.[18] Ovšem některá pravidla ochrany údajů se přesto mohou v řadě situací nepřímo vztahovat i na informace týkající se podniků nebo právnických osob.

Na právnické osoby se vztahují některá ustanovení směrnice 2002/58/ES o soukromí a elektronických komunikacích. V článku 1 této směrnice se uvádí: „2. *Ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES pro účely uvedené v odstavci 1. Navíc poskytují ochranu oprávněných zájmů účastníků, kteří jsou právnickými osobami*.“ V souladu s tím články 12 a 13 rozšiřují použití některých ustanovení o účastnických seznamech a nevyžádaných sděleních i na právnické osoby.

Informace o právnických osobách lze považovat za informace „týkající se“ fyzických osob podle kritérií uvedených v tomto dokumentu také na základě jejich věcného obsahu. Tak tomu může být například tehdy, když je název právnické osoby odvozen od jména fyzické osoby. Dalším příkladem může být podnikový e-mail, který obvykle používá určitý zaměstnanec, nebo informace o malém podniku (který je z právního hlediska „věcí“, a nikoli právnickou osobou), které mohou popisovat chování jeho majitele. Ve všech těchto případech, kdy je na základě kritérií „obsahu“, „účelu“ nebo „výsledku“ možné mít za to, že se informace o právnické osobě nebo podniku „týkají“

---

[17] Zápis ze zasedání Rady Evropské unie konaného dne 8. února 1995, dokument 4730/95: „K čl. 2 písm. a) „*Rada a Komise potvrzují, že stanovení toho, zda a do jaké míry se tato směrnice použije pro zemřelé osoby, přísluší členským státům.*“

[18] 24. bod odůvodnění směrnice: „*vzhledem k tomu, že se tato směrnice nevztahuje na právní předpisy týkající se ochrany právnických osob v souvislosti se zpracováním údajů*“.

fyzické osoby, měly by se považovat za osobní údaje a pravidla ochrany údajů by se měla použít.

Evropský soudní dvůr jasně stanovil, že členským státům nic nebrání, aby oblast působnosti vnitrostátních právních předpisů, kterými se provádí směrnice, rozšířily na oblasti nespadající do její působnosti za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství.[19] V souladu s tím některé členské státy, například Itálie, Rakousko nebo Lucembursko, použití některých ustanovení vnitrostátních právních předpisů přijatých na základě směrnice (například ustanovení o bezpečnostních opatřeních) skutečně rozšířily i na zpracování údajů o právnických osobách.

Stejně jako u informací o zemřelých lidech se i zde může stát, že se v důsledku praktických opatření správce údajů budou pravidla ochrany údajů fakticky vztahovat také na údaje o právnických osobách. Jestliže správce údajů bez rozlišení shromažďuje údaje o fyzických a právnických osobách a ukládá je do stejných datových souborů, mechanismy zpracování údajů a kontrolní systém mohou být navrženy tak, aby vyhovovaly pravidlům ochrany údajů. Ve skutečnosti může být pro správce snazší používat pravidla ochrany údajů pro všechny druhy informací v jeho záznamech než snažit se informace třídit podle toho, zda se týkají fyzických, nebo právnických osob.

IV. CO SE STANE, KDYŽ SE NA ÚDAJE DEFINICE NEVZTAHUJE?

Jak je v tomto dokumentu uvedeno na řadě míst, informace se za různých okolností nemusejí považovat za osobní údaje. To platí v případech, kdy nelze mít za to, že se údaje týkají jednotlivce, nebo kdy jednotlivce nelze považovat za identifikovaného ani identifikovatelného. Jestliže se pojem „osobní údaje“ na zpracovávané informace nevztahuje, důsledkem je, že se směrnice v souladu se svým článkem 3 nepoužije. To ovšem neznamená, že mohou být jednotlivci v dané konkrétní situaci zbaveni jakékoli ochrany. V úvahu je třeba vzít níže uvedené aspekty.

Jestliže se směrnice nepoužije, je možné, že se použijí vnitrostátní právní předpisy o ochraně údajů. Jak stanoví její článek 34, směrnice je určena členským státům. Mimo oblast její působnosti členské státy nepodléhají povinnostem, které ukládá, tj. zejména povinnosti přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Jak ovšem jasně stanovil Evropský soudní dvůr, členským státům nic nebrání, aby oblast působnosti vnitrostátních právních předpisů, kterými se směrnice provádí, rozšířily na oblasti nespadající do její působnosti za předpokladu, že to není v rozporu s žádným jiným právním předpisem Společenství. Může se proto snadno stát, že na některé situace nezahrnující zpracování osobních údajů podle definice ve směrnici se přesto vztahují ochranná opatření podle vnitrostátních právních předpisů. To se může týkat například údajů kódovaných pomocí klíče bez ohledu na to, zda jsou, nebo nejsou osobními údaji.

I v případech, kdy se pravidla ochrany údajů nepoužijí, mohou některé činnosti představovat porušení článku 8 Evropské úmluvy o lidských právech, který chrání právo na soukromý a rodinný život, ve světle rozsáhlé judikatury Evropského soudu pro lidská práva. V případech, kdy se pravidla ochrany údajů nepoužijí, ale v sázce

[19] Rozsudek Evropského soudního dvora ve věci C-101/2001 (Lindqvist) ze dne 6. listopadu 2003, bod 98.

mohou být různé oprávněné zájmy, mohou jednotlivcům poskytnout ochranu i jiné soubory pravidel, jako je právo občanskoprávních deliktů, trestní právo nebo právní předpisy proti diskriminaci.

V. ZÁVĚRY

V tomto stanovisku pracovní skupina poskytuje vodítko ke způsobu, jakým by se měl chápat pojem osobní údaje ve směrnici 95/46/ES a souvisejících právních předpisech Společenství a jak by se měl v různých situacích používat.

V rámci obecných úvah bylo konstatováno, že evropský zákonodárce měl v úmyslu zavést široký pojem osobní údaje, jehož rozsah však není neomezený. Stále je třeba mít na paměti, že cílem pravidel obsažených ve směrnici je ochrana základních práv a svobod jednotlivců, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů. Tato pravidla byla proto vytvořena pro použití v situacích, kdy mohou být práva jednotlivců ohrožena, a kdy tudíž potřebují ochranu. Oblast působnosti pravidel ochrany údajů by se neměla nadměrně rozšiřovat, ale současně je třeba se vyvarovat nepatřičnému zužování pojmu osobní údaje. Směrnice vymezuje oblast své působnosti, z níž vylučuje řadu činností, a u činností, které do její oblasti působnosti spadají, umožňuje pružné používání pravidel. Zásadní úlohu při hledání vhodné rovnováhy v jejich používání hrají orgány pro ochranu údajů (viz oddíl II).

Analýza pracovní skupiny vychází ze čtyř hlavních složek, které lze rozlišit v definici „osobních údajů“: „veškeré informace“, „o“ (vztah mezi informacemi a osobou), „identifikovaná nebo identifikovatelná“ a (fyzická) „osoba“. Tyto složky jsou těsně provázány a vzájemně se podporují a společně rozhodují o tom, zda by se určitá informace měla považovat za „osobní údaj“. Na podporu uvedené analýzy byly využity příklady z vnitrostátní praxe evropských orgánů pro ochranu údajů.

- První složka – „veškeré informace“ – vyžaduje široký výklad pojmu osobní údaje – nezávisle na povaze a obsahu informací a technickém formátu, ve kterém jsou prezentovány. To znamená, že za „osobní údaje“ lze považovat jak objektivní, tak subjektivní informace o osobě v libovolném postavení, a to bez ohledu na to, jaký technický nosič je obsahuje. Stanovisko se zabývá také biometrickými údaji a právním rozdílem mezi nimi a vzorky lidských tkání, z nichž se dají získat (viz oddíl III bod 1).

- Druhá složka – „o“ (vztah mezi informacemi a osobou) – byla dosud často přehlížena, ale přitom má klíčový význam pro určení věcného rozsahu dotčeného pojmu, zejména ve vztahu k věcem a novým technologiím. Stanovisko předkládá tři alternativní prvky, tj. obsah, účel nebo výsledek, umožňující určit, zda je informace „o“ jednotlivci (týká se jednotlivce). To se týká také informací, které mohou mít zjevný dopad na způsob, jakým se s jednotlivcem zachází nebo jakým je hodnocen (viz oddíl III bod 2).

- Třetí složka – „identifikovaná nebo identifikovatelná“ – je posouzena se zaměřením na podmínky, za kterých má být jednotlivec považován za „identifikovatelného“, a zvláště na „prostředky, které mohou být rozumně použity“ správcem nebo jakoukoli jinou osobou k jeho identifikaci. V této analýze hrají důležitou úlohu konkrétní souvislosti a okolnosti každého případu. Stanovisko se zabývá také „pseudonymizovanými údaji“ a použitím „údajů kódovaných pomocí klíče“ ve statistických šetřeních nebo farmaceutickém výzkumu (viz oddíl III bod 3).

- Čtvrtá složka – (fyzická) „osoba“ – je analyzována s ohledem na požadavek, že „osobní údaje“ musejí být o „žijících jednotlivcích“. Stanovisko se věnuje rovněž oblastem, které hraničí s údaji o zemřelých osobách, nenarozených dětech a právnických osobách (viz oddíl III bod 4).

Nakonec se ve stanovisku řeší otázka, co se stane, když se definice „osobních údajů“ na údaje nevztahuje. V takových případech mohou být k dispozici různá řešení, včetně vnitrostátních právních předpisů, které při dodržení ostatních právních předpisů Společenství mohou zasahovat i mimo oblast působnosti směrnice (viz oddíl IV).

Pracovní skupina vyzývá všechny zúčastněné strany, aby pečlivě prostudovaly pokyny obsažené v tomto stanovisku a braly je v potaz při výkladu a používání vnitrostátních právních předpisů v souladu se směrnicí 95/46/ES.

Členové pracovní skupiny, kteří jsou většinou představiteli vnitrostátních orgánů dozoru nad ochranou údajů, jsou odhodláni pokyny poskytnuté v tomto stanovisku dále rozvíjet v rámci oblastí svých pravomocí a zajišťovat řádné používání vnitrostátních právních předpisů svých zemí v souladu se směrnicí 95/46/ES.

Pracovní skupina má v úmyslu pokyny obsažené v tomto stanovisku uplatňovat a rozvíjet ve všech vhodných oblastech a pečlivě je zohledňovat ve své další práci, zejména při řešení otázek, jako je správa identit v rámci elektronické veřejné správy a elektronického zdravotnictví, jakož i v souvislosti s identifikací na základě rádiové frekvence (RFID). U druhého z uvedených témat pracovní skupina zamýšlí přispět k další analýze dopadu, jaký pravidla ochrany údajů mohou mít na využití RFID, a případných dodatečných opatření, která mohou být nezbytná k zajištění řádného respektování práv a zájmů na ochranu údajů v této oblasti.

Konečně by pracovní skupina také přivítala jakoukoli zpětnou vazbu od zúčastněných stran a orgánů dozoru ohledně jejich praktických zkušeností s pokyny v tomto stanovisku, včetně případných dalších příkladů vedle těch, které jsou uvedeny v tomto dokumentu. Skupina má v úmyslu se k tomuto tématu ve vhodné době vrátit s cílem dále posílit společné porozumění klíčovému pojmu osobní údaje a na tomto základě zajistit harmonizované používání a lepší provádění směrnice 95/46/ES a souvisejících právních předpisů Společenství.

Za pracovní skupinu

Peter SCHAAR
předseda