PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

01248/07/SK
WP 136

Stanovisko 4/2007 k pojmu osobné údaje

Prijaté 20. júna

Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom pre ochranu údajov a súkromia. Jej úlohy sú definované v článku 30 smernice 95/46/ES a článku 15 smernice 2002/58/ES.

Úlohy sekretariátu plní riaditeľstvo C (Občianske právo, základné práva a občianstvo) Európskej komisie, Generálne riaditeľstvo pre spravodlivosť, slobodu a bezpečnosť, B-1049 Brusel, Belgicko, kancelária č. LX-46 01/43.

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

PRACOVNÁ SKUPINA PRE OCHRANU JEDNOTLIVCOV V SÚVISLOSTI SO SPRACOVANÍM OSOBNÝCH ÚDAJOV

zriadená podľa smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995[1],

so zreteľom na články 29 a 30 ods. 1 písm. a) a ods. 3 tejto smernice a článok 15 odsek 3 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002,

so zreteľom na článok 255 Zmluvy o ES a nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie,

so zreteľom na rokovací poriadok,

PRIJALA TOTO STANOVISKO:

[1] Úradný vestník ES L 281, 23.11.1995, s. 31, k dispozícii na internetovej adrese: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. ÚVOD

Pracovná skupina si uvedomuje potrebu vykonať dôkladnú analýzu pojmu osobné údaje. Informácie o súčasnej praxi v členských štátoch EÚ svedčia o tom, že medzi členskými štátmi je určitá neistota a určitá odlišnosť v praxi, pokiaľ ide o dôležité aspekty tohto pojmu, ktoré môžu v rôznych kontextoch ovplyvniť riadne fungovanie existujúceho rámca ochrany údajov. Výsledky tejto analýzy hlavného prvku uplatňovania a výkladu pravidiel ochrany údajov budú mať značný vplyv na mnohé dôležité otázky a budú sa osobitne týkať tém, medzi ktoré patrí správa identity v rámci elektronickej štátnej správy a elektronického zdravotníctva, ako aj v rámci rádiofrekvenčnej identifikácie (Radio Frequency Identification, RFID).

Cieľom tohto stanoviska pracovnej skupiny je dospieť k spoločnému výkladu pojmu osobné údaje, situácií, v ktorých by sa mali uplatňovať vnútroštátne právne predpisy o ochrane údajov, a spôsobu, akým by sa mali uplatňovať. Práca na spoločnej definícii pojmu osobné údaje sa rovná definovaniu toho, čo patrí a čo nepatrí do rozsahu pôsobnosti pravidiel o ochrane údajov. Cieľom tejto práce je vypracovať usmernenie o spôsobe, akým by sa vnútroštátne pravidlá o ochrane údajov mali uplatňovať na určité kategórie situácií, ktoré nastávajú v celej Európe. Takto prispeje pracovná skupina zriadená podľa článku 29 k jednotnému uplatňovaniu takýchto noriem, čo je jednou z jej hlavných úloh.

Tento dokument využíva príklady z vnútroštátnej praxe európskych orgánov na ochranu údajov (Data Protection Authorities, DPA) s cieľom podporiť a objasniť túto analýzu. Väčšina príkladov sa upravila iba na účely ich primeraného využitia v tejto súvislosti.

II. VŠEOBECNÉ ÚVAHY A POLITICKÉ OTÁZKY

Široké poňatie pojmu osobné údaje v smernici

Definícia osobných údajov uvedená v smernici 95/46/ES (ďalej len smernica o ochrane údajov“ alebo „smernica“) znie takto:

„Osobné údaje znamenajú akúkoľvek informáciu, ktorá sa týka identifikovanej alebo identifikovateľnej fyzickej osoby („údajového subjektu“); identifikovateľná osoba je osoba, ktorú možno identifikovať, priamo alebo nepriamo, najmä pomocou overenia identifikačného čísla alebo jedného alebo viacerých faktorov špecifických pre jeho fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu“.

Je potrebné uviesť, že v tejto definícii sa odráža zámer európskeho zákonodarcu o širší pojem „osobných údajov“, ktorý sa zachoval počas celého legislatívneho procesu. V pôvodnom návrhu Komisie bolo vysvetlené, že „*rovnako ako v dohovore 108 sa prijíma široká definícia, aby sa vzťahovala na všetky informácie, ktoré sa môžu spájať s jednotlivcom*“[2]. V upravenom návrhu Komisie bolo uvedené, že *„zmenený a doplnený návrh spĺňa želanie Parlamentu, aby definícia „osobných údajov“ bola čo najvšeobecnejšia, aby zahŕňala všetky informácie týkajúce sa identifikovateľného jednotlivca*“[3], želanie, ktoré v spoločnom stanovisku[4] zohľadnila aj Rada.

Cieľom pravidiel uvedených v smernici je chrániť jednotlivcov.

V článku 1 smernice 95/46/ES a v článku 1 smernice 2002/58/ES sa jasne stanovuje hlavný účel pravidiel obsiahnutých v uvedených dokumentoch: chrániť základné práva a slobody fyzických osôb a najmä ich právo na súkromie, pokiaľ ide o spracovanie osobných údajov. Je to veľmi dôležitý prvok, ktorý sa musí zohľadniť pri výklade a uplatňovaní pravidiel oboch nástrojov. Môže zohrávať podstatnú úlohu pri stanovení, ako uplatňovať ustanovenia smernice v mnohých situáciách, v ktorých nie sú ohrozené práva jednotlivcov, a môže varovať pred akýmkoľvek výkladom týchto pravidiel, ktoré by zbavili jednotlivcov ochrany ich práv.

Z rozsahu pôsobnosti smernice je vylúčených niekoľko činností a v jej znení je určitá flexibilita, aby sa zabezpečila primeraná právna reakcia na príslušné okolnosti

Napriek širokému poňatiu pojmov „osobné údaje“ a „spracovanie“, ktoré sú obsiahnuté v smernici, skutočnosť, že určitá situácia sa môže považovať za situáciu, ktorá zahŕňa „spracovanie osobných údajov“ v zmysle definície, sama o sebe neznamená, že táto situácia podlieha pravidlám smernice, najmä podľa jej článku 3. Okrem výnimiek v dôsledku pôsobnosti právnych predpisov Spoločenstva, výnimky podľa článku 3 zohľadňujú technický spôsob spracovania (manuálnou neštruktúrovanou formou) a zámer využitia (na výlučne osobné činnosti alebo činnosti týkajúce sa domácnosti vykonávané fyzickou osobou). Dokonca aj v prípade, že ide o spracovanie osobných údajov v rámci rozsahu pôsobnosti smernice, nemusia byť v konkrétnom prípade

[2] KOM (90) 314 v konečnom znení, 13.9.1990, s. 19 (komentár k článku 2).
[3] KOM (92) 422 v konečnom znení, 28.10.1992, s. 10 (komentár k článku 2).
[4] Spoločné stanovisko (ES) č. 1/95 prijaté Radou 20. februára 1995, Ú. v. ES C 93, 13.4.1995, s. 20.

uplatniteľné všetky pravidlá uvedené v tejto smernici. Niektoré ustanovenia smernice obsahujú značný stupeň flexibility, aby sa dosiahla primeraná rovnováha medzi ochranou práv údajového subjektu na jednej strane a zákonnými záujmami kontrolórov údajov, tretích strán a možným verejným záujmom na strane druhej. Niektoré príklady takýchto ustanovení sú uvedené v článku 6 (doba uchovávania v závislosti od údajov, ktoré sú potrebné), článku 7 písm. f) (rovnováha záujmov opodstatňujúcich spracovanie), v poslednom odseku článku 10 písm. c) a článku 11 ods. 1 písm. c) (informovanie údajového subjektu, aby sa zaručilo riadne spracovávanie), alebo v článku 18 (výnimky z oznamovacej povinnosti), ak uvedieme iba niekoľko prípadov.

Rozsah pôsobnosti pravidiel o ochrane údajov by sa nemal nadmerne rozširovať

Uplatňovanie pravidiel o ochrane údajov v situáciách, v prípade ktorých nebolo zámerom, aby sa na ne vzťahovali uvedené pravidlá a na ktoré zákonodarca pravidlá nevypracoval, by bolo neželaným výsledkom. Uvedené vecné výnimky podľa článku 3 a v odôvodneniach 26 a 27 smernice prezentujú ako zákonodarca chcel, aby sa realizovala ochrana údajov.

Jedno obmedzenie sa týka spôsobu spracovania údajov. Je užitočné pripomenúť, že dôvodom uzákonenia prvých právnych predpisov o ochrane údajov v sedemdesiatych rokoch bola nová technológia vo forme elektronického spracovania údajov umožňujúca ľahší a širší prístup k osobným údajom ako v prípade tradičných foriem spracovania údajov. V dôsledku toho sa ochrana údajov podľa smernice zameriava na ochranu takých foriem spracovania, ktoré sa vyznačujú vyšším rizikom umožnenia „ľahkého prístupu k osobným údajom“ (odôvodnenie 27). Spracovanie osobných údajov neautomatickými prostriedkami je zahrnuté do rozsahu pôsobnosti smernice iba vtedy, ak údaje tvoria súčasť registračného systému alebo sú určené na to, aby tvorili súčasť takéhoto systému (článok 3).

Ďalším všeobecným obmedzením uplatňovania ochrany údajov podľa smernice by bolo spracovanie údajov za okolností, keď nie je „primeraná pravdepodobnosť, že ich využije“ nejaká osoba (odôvodnenie 26), čo je problém, ktorým sa budeme zaoberať neskôr.

Je však potrebné vyhnúť sa aj nevhodnému obmedzeniu výkladu pojmu osobné údaje.

V prípadoch, v ktorých by mechanické uplatňovanie každého jedného ustanovenia smernice na prvý pohľad viedlo k nadmerne obtiažnym alebo možno dokonca absurdným dôsledkom, je nutné najprv skontrolovať: 1) či situácia patrí do pôsobnosti smernice, najmä v súlade s jej článkom 3; a 2) v prípade, že patrí do jej pôsobnosti, či samotná smernica alebo vnútroštátne právne predpisy prijaté podľa nej neumožňujú výnimky alebo zjednodušenia, pokiaľ ide o konkrétne situácie, aby sa dosiahla primeraná právna reakcia pri zabezpečení ochrany práv a záujmov jednotlivca. Lepšou možnosťou je vyhnúť sa neprimeranému obmedzovaniu výkladu definície osobných údajov a radšej si uvedomiť, že pri uplatňovaní pravidiel na údaje existuje značná flexibilita.

V tomto zmysle zohrávajú dôležitú úlohu vnútroštátne dozorné orgány pre ochranu údajov, ktoré majú na starosti monitorovanie uplatňovania právnych predpisov o ochrane údajov, čo zahŕňa aj poskytovanie výkladu právnych ustanovení a vypracovávanie konkrétneho usmernenia pre kontrolórov a pre údajové subjekty.

Mali by usilovať o takú definíciu, ktorá je dosť široká, aby mohla predvídať vývoj a v rámci svojej pôsobnosti zachytiť všetky „šedé zóny“ a pri tom zákonne využívať flexibilitu obsiahnutú v smernici. Text smernice v skutočnosti vyzýva k rozvíjaniu politiky, v ktorej sa spája široký výklad pojmu osobné údaje s primeranou rovnováhou pri uplatňovaní pravidiel smernice.

III. ANALÝZA DEFINÍCIE „OSOBNÝCH ÚDAJOV“ PODĽA SMERNICE O OCHRANE ÚDAJOV

Definícia v smernici obsahuje štyri hlavné zložky, ktoré sa na účely tohto dokumentu budú analyzovať samostatne. Sú to tieto zložky:

- „akékoľvek informácie“
- „týkajúce sa“
- „identifikovaná a identifikovateľná“
- „fyzická osoba“.

Tieto štyri zložky sú úzko prepojené a navzájom sa dopĺňajú. V záujme metodológie, ktorá sa má v tomto dokumente dodržiavať, sa však každou z týchto položiek budeme zaoberať samostatne.

1. PRVÝ PRVOK: „AKÉKOĽVEK INFORMÁCIE“

Pojem „akékoľvek informácie“ uvedený v smernici jasne signalizuje ochotu zákonodarcu vytvoriť širokú definíciu pojmu osobné údaje. Táto formulácia si vyžaduje širší výklad.

Z hľadiska charakteru informácií zahŕňa pojem osobné údaje akýkoľvek druh údajov o osobe. Vzťahuje sa na „objektívne“ informácie, napríklad, prítomnosť určitej látky v krvi osoby. Zahŕňa aj „subjektívne“ informácie, názory alebo hodnotenia. Tento subjektívny druh informácií tvorí značnú časť osobných údajov spracovávaných v sektoroch, medzi ktoré patrí bankovníctvo, s cieľom posúdiť spoľahlivosť dlžníkov („Titius je spoľahlivý dlžník“), poisťovníctvo („očakáva sa, že Titius nezomrie skoro“) alebo oblasť zamestnania („Titius je dobrý pracovník a zaslúži si povýšenie“).

Informácie nemusia byť pravdivé alebo preukázané, aby ich bolo možné označiť za „osobné údaje“. Pravidlá o ochrane údajov v skutočnosti už počítajú s možnosťou, že informácie sú nesprávne a poskytujú údajovému subjektu právo na prístup k uvedeným informáciám a vznesenie námietok prostredníctvom primeraných opravných prostriedkov[5].

Z hľadiska obsahu informácií pojem osobné údaje zahŕňa údaje poskytujúce akýkoľvek druh informácií. Patria sem samozrejme osobné informácie považované za „citlivé údaje“ podľa článku 8 smernice v dôsledku ich osobitne rizikového charakteru, ale aj všeobecnejšie druhy informácií. Pojem „osobné údaje“ zahŕňa informácie týkajúce sa „stricto sensu“ súkromného a rodinného života jednotlivca, ale aj informácie, ktoré sa týkajú akýchkoľvek druhov činnosti, ktoré vykonáva jednotlivec, napríklad činnosti

[5] Náprava by sa mohla uskutočniť pridaním opačných pripomienok alebo využitím primeraných opravných prostriedkov, medzi ktoré patria odvolacie mechanizmy.

týkajúcej sa pracovných vzťahov alebo ekonomického alebo sociálneho správania jednotlivca. Zahŕňa preto informácie o jednotlivcoch bez ohľadu na postavenie alebo funkciu týchto osôb (ako spotrebiteľa, pacienta, zamestnanca, zákazníka, atď.).

Príklad č. 1: Profesné zvyklosti a praktiky

Informácie o lekárskom predpise (napríklad, identifikačné číslo lieku, názov lieku, účinnosť lieku, výrobca, predajná cena, nové alebo doplniteľné balenie, dôvody na užívanie, dôvody na príkaz o nemožnosti nahradenia lieku, meno a priezvisko lekára, ktorý predpísal liek, telefónne číslo atď.), či už vo forme individuálneho predpisu alebo vo forme vzorov odlíšených od mnohých predpisov, sa môžu považovať za osobné údaje o lekárovi, ktorý predpisuje tento liek, aj keď je pacient anonymný. Poskytovanie informácií o lekárskych predpisoch, ktoré napísali identifikovaní a identifikovateľní lekári, výrobcom liekov na predpis je teda oznámenie osobných údajov tretím stranám v zmysle smernice.

Tento výklad podporuje znenie samotnej smernice. Na jednej strane sa musí zohľadniť, že pojem súkromný a rodinný život je široký, ako objasnil Európsky súd pre ľudské práva[6]. Pravidlá o ochrane osobných údajov na druhej strane idú nad rámec ochrany širokého poňatia pojmu právo na rešpektovanie súkromného a rodinného života. Je nutné uviesť, že v Charte základných práv Európskej únie je ochrana osobných údajov zakotvená v článku 8 ako autonómne právo oddelené a odlišné od práva na súkromný život uvedeného v jej článku 7, a to isté platí na vnútroštátnej úrovni v niektorých členských štátoch. Zodpovedá to podmienkam uvedeným v článku 1 ods. 1, ktoré sú zamerané na ochranu „základných práv a slobôd fyzických osôb, a *najmä* [ale nie výhradne] ich práva na súkromie“. V smernici sa preto uvádza osobitný odkaz na spracovanie osobných údajov v kontextoch netýkajúcich sa domova a rodiny, medzi ktoré patrí spracovanie údajov v pracovnoprávnej oblasti (článok 8 ods. 2 písm. b)), v trestnoprávnej oblasti, v oblasti administratívnych sankcií alebo rozsudkov v občianskoprávnych prípadoch (článok 8 ods. 5) alebo priameho marketingu (článok 14 písm. b)). Európsky súdny dvor[7] potvrdil tento široký prístup.

Pokiaľ ide o formát alebo médium, na ktorom sa uvedené informácie uchovávajú, zahŕňa pojem osobné údaje informácie, ktoré sú k dispozícii v akejkoľvek forme, či už abecednej, číselnej, grafickej, fotografickej alebo zvukovej. Zahŕňa informácie uchovávané na papieri, ako aj informácie uchovávané v pamäti počítača vo forme binárneho kódu alebo napríklad na videopáske. Je to logický dôsledok pokrytia automatického spracovania osobných údajov v rámci jeho rozsahu. Najmä zvukové a obrazové údaje je potrebné pokladať za osobné údaje, pretože môžu predstavovať informácie o jednotlivcovi. Z tohto hľadiska sa osobitný odkaz na zvukové a obrazové údaje v článku 33 smernice musí chápať ako potvrdenie a objasnenie, že tento druh

[6] Rozsudok Európskeho súdu pre ľudské práva v prípade Amann vs Švajčiarsko zo 16.2.2000, §65 : *„[...] pojem „súkromný život“ sa nesmie vykladať obmedzujúcim spôsobom. Rešpektovanie súkromného života zahŕňa najmä právo vytvárať a rozvíjať vzťahy s inými ľuďmi; okrem toho neexistuje žiadny dôvod na zásadu odôvodňovať vylúčenie činností profesnej alebo obchodnej povahy z pojmu „súkromný život“ (pozri rozsudok Niemietz vs Nemecko zo 16. decembra 1992, séria A č. 251-B, strany 33 - 34, § 29, a už citovaný rozsudok Halford, strany 1015 - 1016, § 42). Uvedený široký výklad zodpovedá výkladu dohovoru Rady Európy z 28. januára 1981 [...]“.*

[7] Rozsudok Európskeho súdneho dvora C-101/2001 zo 6.11.2003 (Lindqvist), §24: „*Pojem osobné údaje používaný v článku 3 ods. 1 smernice 95/46 sa podľa definície v jej článku 2 písm. a) vzťahuje na akúkoľvek informáciu týkajúcu sa identifikovanej alebo identifikovateľnej fyzickej osoby. Pojem sa nepochybne vzťahuje na meno osoby v spojitosti s jej telefónnym číslom alebo informáciami o jej pracovných podmienkach alebo záľubách“.*

údajov skutočne patrí do rozsahu jej pôsobnosti (za predpokladu, že sú splnené všetky ostatné podmienky) a že sa táto smernica na ne vzťahuje. Je to logický predpoklad týkajúci sa ustanovenia uvedeného v tomto článku, ktorý sa snaží posúdiť, či pravidlá smernice poskytujú v uvedených oblastiach primerané právne reakcie. Táto skutočnosť je ďalej objasnená v odôvodnení 14, v ktorom sa uvádza, že „*vzhľadom na význam neustáleho vývoja činností v rámci informačnej spoločnosti, metód používaných na zber, prenos, manipuláciu, záznam alebo komunikovanie zvukových a obrazových údajov vo vzťahu k fyzickým osobám, by sa táto smernica mala týkať spracovania vrátane zahrnutia týchto údajov*“. Na druhej strane nie je nutné, aby sa za osobné údaje považovali informácie, ktoré sú obsiahnuté v štruktúrovanej databáze alebo súbore. Za osobné údaje sa môžu pokladať aj informácie obsiahnuté vo voľnom texte v elektronickom dokumente za predpokladu, že sú splnené ostatné kritériá definície osobných údajov. „Osobné údaje“ môžu byť napríklad obsiahnuté v správe elektronickej pošty .

Príklad č. 2: Telefónbanking:

V prípade telefónbankingu, pri ktorom sa hlas zákazníka, ktorý dáva banke pokyny, nahráva na pásku, by sa takéto nahrané pokyny mali považovať za osobné údaje.

Príklad č. 3: Videomonitorovanie

Obrazy osôb zachytených systémom videomonitorovania môžu byť osobnými údajmi, pokiaľ sú jednotlivci rozpoznateľní.

Príklad č. 4: Detská kresba

Výsledkom neurologicko-psychiatrického testu uskutočneného s dievčatkom je kresba, na ktorej dievča zobrazilo svoju rodinu. Táto kresba sa predkladá v rámci súdneho konania vo veci jej opatrovníctva. Kresba poskytuje informácie o nálade dievčaťa a jeho pocitoch k rôznym príslušníkom rodiny. Kresba ako taká sa môže považovať za „osobné údaje“. V skutočnosti odhaľuje informácie týkajúce sa dieťaťa (jeho zdravotný stav z psychiatrického hľadiska) a tiež napríklad informácie o správaní jeho otca alebo matky. V dôsledku toho môžu rodičia v uvedenom prípade uplatňovať svoje právo na prístup k tejto osobitnej informácii.

Osobitne je potrebné spomenúť biometrické údaje. Tieto údaje možno definovať ako biologické vlastnosti, fyziologické znaky, črty alebo opakovateľné činnosti, v prípade ktorých sú tieto vlastnosti a/alebo činnosti špecifické pre uvedeného jednotlivca a zároveň merateľné, aj keď spôsoby používané v praxi na ich technické meranie zahŕňajú určitý stupeň pravdepodobnosti. Typickým príkladom takýchto biometrických údajov sú odtlačky prstov, sietnica, tvar tváre, hlas, ale aj geometria ruky, štruktúry žíl alebo dokonca určitá hlboko zakorenená schopnosť alebo iná vlastnosť týkajúca sa správania (napríklad, vlastnoručný podpis, údery na klávesnici, osobitný spôsob chôdze alebo reči atď.).

Osobitosť biometrických údajov spočíva v tom, že tieto údaje sa môžu pokladať za *obsah* informácií o konkrétnom jednotlivcovi (Titius má tieto odtlačky prstov), ako aj za prvok na vytvorenie *spojenia* medzi informáciou a jednotlivcom (tohto predmetu sa dotkol niekto, komu patria tieto odtlačky prstov, a tieto odtlačky prstov zodpovedajú odtlačkom prstov Titia; tohto predmetu sa preto dotkol Titius). Tieto informácie ako také môžu slúžiť ako „identifikátory“. Biometrické údaje sa môžu vzhľadom na ich jedinečnú súvislosť s konkrétnym jednotlivcom používať na identifikáciu jednotlivca.

Tento duálny charakter sa objavuje aj v prípade údajov o DNA, ktoré poskytujú informácie o ľudskom tele a umožňujú jednoznačnú a jedinečnú identifikáciu osoby.

Vzorky ľudských tkanív (napríklad vzorka krvi) sú zdrojmi biometrických údajov, ale samé o sebe nie sú biometrickými údajmi (napríklad odtlačok prsta je biometrickým údajom, ale prst samotný nie je biometrickým údajom). Získavanie informácií zo vzoriek je preto zhromažďovaním osobných údajov, na ktoré sa vzťahujú pravidlá smernice. Zhromažďovanie, uchovávanie a využívanie samotných vzoriek tkanív môže podliehať samostatným súborom pravidiel[8].

2. DRUHÝ PRVOK: „TÝKAJÚCE SA“

Definícia tohto prvku je zásadná, pretože je veľmi dôležité presne zistiť ktoré vzťahy/spojenia sú podstatné, a ako ich rozlišovať.

Informácie sa vo všeobecnosti môžu pokladať za informácie, ktoré sa „týkajú“ jednotlivca, ak sú *o* uvedenom jednotlivcovi.

Tento vzťah sa dá v mnohých situáciách ľahko určiť. Napríklad údaje nachádzajúce sa v individuálnom súbore osoby na personálnom oddelení sa jasne „týkajú“ zamestnaneckého postavenia osoby. Rovnako aj údaje o výsledkoch lekárskych vyšetrení pacienta uvedené v jeho zdravotných záznamoch alebo obraz osoby na videozázname z pohovoru s uvedenou osobou.

Je však možné uviesť mnoho ďalších situácií, v ktorých nie je určenie, že informácie sa „týkajú“ jednotlivca, vždy tak evidentné ako v predchádzajúcich prípadoch.

V niektorých prípadoch sa informácie poskytované údajmi týkajú predovšetkým vecí a nie jednotlivcov. Tieto veci zvyčajne niekomu patria alebo môžu podliehať osobitnému vplyvu jednotlivcov, alebo naopak vplývať na jednotlivcov, alebo môžu zachovávať určitý druh fyzickej alebo geografickej blízkosti s jednotlivcami alebo s inými vecami. Potom sa môže iba nepriamo uvažovať o tom, že informácie sa týkajú uvedených jednotlivcov alebo uvedených vecí.

Príklad č. 5: Hodnota domu

Hodnota konkrétneho domu je informáciou o veci. Je zrejmé, že pravidlá o ochrane údajov sa nebudú uplatňovať v prípadoch, keď sa takáto informácia bude používať iba na uvedenie príkladu úrovne cien nehnuteľností v určitom okrese. Za určitých okolností by sa však takéto informácie mali považovať aj za osobné údaje. Dom je v skutočnosti majetkom vlastníka, ktorý sa takto použije na stanovenie rozsahu povinnosti tejto osoby, napríklad v súvislosti s platením daní. Z tohto hľadiska bude nepopierateľné, že takéto informácie by sa mali pokladať za osobné údaje.

Podobnú analýzu možno uplatniť aj v prípade, keď sa údaje týkajú predovšetkým postupov alebo udalostí, napríklad informácie o fungovaní stroja, ktorý obsluhuje nejaká osoba. Za určitých okolností sa tieto informácie môžu tiež považovať za informácie „týkajúce sa“ jednotlivca.

Príklad č. 6: Záznamy o opravách auta

[8] Pozri odporúčanie Výboru ministrov Rady Európy č. Rec (2006) 4 členským štátom týkajúce sa výskumu biologických materiálov ľudského pôvodu z 15.3.2006.

Záznamy o opravách auta, ktoré vedie mechanik alebo autoopravovňa, obsahujú informácie o aute, najazdených kilometroch, dátumoch servisných kontrol, technických problémoch a stave materiálu. Tieto informácie sa zapisujú do záznamov k údajom, ako je poznávacia značka auta a číslo motora, ktoré je zasa možné dať do súvislosti s vlastníkom auta. V prípade, že autoopravovňa uvedie do súvislosti vozidlo a vlastníka na účely fakturácie, informácie sa budú „týkať“ vlastníka alebo vodiča. Ak sa vytvorí súvislosť s automechanikom, ktorý pracoval na aute, na účely zistenia jeho produktivity, táto informácia sa bude „týkať“ tiež automechanika.

Pracovná skupina už venovala pozornosť otázke, kedy sa môžu informácie považovať za informácie „týkajúce sa“ osoby. V rámci diskusií o otázkach ochrany údajov, ktoré vyvolali štítky RFID, pracovná skupina uviedla, že *„údaje sa týkajú jednotlivca, ak sa týkajú totožnosti, charakteristík alebo správania jednotlivca, alebo ak sa takéto informácie používajú na určenie alebo ovplyvnenie spôsobu, akým sa s uvedenou osobou zaobchádza alebo akým sa uvedená osoba posudzuje*[9].“

Vzhľadom na uvedené prípady by sa rovnako mohlo zdôrazniť, že aby sa údaje pokladali za údaje „týkajúce sa“ jednotlivca, mal by byť prítomný prvok „**obsahu**“ ALEBO prvok „**účelu**“ ALEBO prvok „**výsledku**“.

Prvok „**obsahu**“ je prítomný v prípadoch, keď sa v súlade s najzrejmejším a najobvyklejším chápaním pojmu „týkajúce sa“ v spoločnosti poskytujú informácie o konkrétnej osobe, bez ohľadu na účel na strane kontrolóra údajov alebo tretej strany, alebo na vplyv uvedenej informácie na údajový subjekt. Informácie sa „týkajú“ osoby, keď sú „o“ uvedenej osobe a túto skutočnosť je potrebné posudzovať z hľadiska všetkých okolností týkajúcich sa prípadu. Napríklad výsledky lekárskej analýzy sa jasne týkajú pacienta, alebo informácie uvedené v spise spoločnosti pod menom určitého klienta sa jasne týkajú tohto klienta. Alebo informácie uvedené na štítku RFID alebo čiarovom kóde v preukaze totožnosti určitého jednotlivca sa týkajú uvedenej osoby, ako v prípade budúcich cestovných pasov s čipom RFID.

Aj prvok „**účelu**“ môže mať za následok, že informácie sa „týkajú“ určitej osoby. Prvok „účelu“ možno pokladať za prítomný, ak sa údaje používajú alebo je pravdepodobné, že sa budú používať, pri zohľadnení všetky okolnosti týkajúcich sa konkrétneho prípadu, na účel posúdenia jednotlivca, zaobchádzania s jednotlivcom určitým spôsobom alebo ovplyvnenia postavenia alebo správania jednotlivca.

Príklad č. 7: Záznamy o telefonických hovoroch

Záznamy o telefonických hovoroch vykonaných z aparátu v kancelárii spoločnosti poskytuje informácie o hovoroch uskutočnených z telefónu v tejto kancelárii spojeného s určitou linkou. Uvedené informácie sa môžu uviesť do vzťahu s rôznymi subjektmi. Na jednej strane bola linka sprístupnená spoločnosti a spoločnosť je na základe zmluvy povinná platiť za tieto hovory. Telefónny aparát je počas pracovnej doby pod kontrolou určitého zamestnanca a predpokladá sa, že tieto hovory vykonáva tento zamestnanec. Záznamy o telefonických hovoroch môžu poskytnúť aj informácie o osobe, ktorá bola volaná. Telefón môže použiť aj ktorákoľvek iná osoba, ktorá má prístup do budovy v neprítomnosti zamestnanca (napríklad upratovací personál). Informácie o používaní uvedeného telefónneho aparátu je možné dať do súvislosti so

[9] Dokument pracovnej skupiny č. WP 105: „Pracovný dokument o otázkach ochrany údajov týkajúcich sa technológie RFID“, prijatý 19.1.2005, s. 8.

spoločnosťou, zamestnancom alebo upratovacím personálom aj na iné účely (napríklad na kontrolu času, kedy upratovací personál opustil pracovisko, keďže musí telefonicky potvrdiť, o ktorej odchádza predtým, ako sa uzamkne budova). Je nutné uviesť, že koncept osobných údajov sa v tomto prípade rozširuje na odchádzajúce aj prichádzajúce hovory, pretože všetky obsahujú informácie týkajúce sa súkromného života, sociálnych vzťahov a komunikácie ľudí.

Tretí druh pojmu „týkajúci sa“ špecifických osôb sa opiera o prítomnosť prvku „**výsledok**“. Napriek neprítomnosti prvku „obsah“ alebo „účel“ sa údaje môžu považovať za údaje „týkajúce sa“ jednotlivca, pretože je pravdepodobné, že ich používanie bude mať dosah na práva a záujmy určitej osoby, pri zohľadnení všetkých okolností týkajúcich sa konkrétneho prípadu. Je potrebné uviesť, že nie je nutné, aby potenciálny výsledok bol hlavným dosahom. Stačí, ak spracovanie takýchto údajov spôsobí, že sa s jednotlivcom môže zaobchádzať inak než s inými osobami.

Príklad č. 8: Monitorovanie pozície taxíkov na optimalizovanie služby, ktoré má vplyv na vodičov

Spoločnosť poskytujúca služby taxíkov zaviedla satelitný systém zisťovania polohy taxíkov s cieľom určiť miesto, na ktorom sa v reálnom čase nachádza dostupný taxík. Účelom spracovania je poskytovať lepšiu službu a ušetriť palivo tým, že každému klientovi, ktorý si objedná taxík, sa pridelí taxík, ktorý je najbližšie k adrese klienta. Presnejšie povedané údaje, ktoré uvedený systém potrebuje, sú údajmi, ktoré sa týkajú áut, nie vodičov. Účelom spracovania nie je posúdiť výkon vodičov taxíkov, napríklad prostredníctvom optimalizácie ich trás. Systém však umožňuje monitorovať výkon vodičov taxíkov a kontrolovať, či dodržiavajú obmedzenia rýchlosti, hľadajú najvhodnejšiu trasu, či sú za volantom alebo oddychujú mimo atď. Môže mať preto značný dosah na týchto jednotlivcov a údaje ako také sa môžu považovať za údaje, ktoré sa týkajú aj fyzických osôb. Spracovanie by malo podliehať pravidlám o ochrane údajov.

Tieto tri prvky (obsah, účel, výsledok) sa musia považovať za alternatívne a nie za kumulatívne podmienky. Najmä ak je prítomný prvok obsahu, nie je potrebná prítomnosť ostatných prvkov, aby sa informácie považovali za informácie týkajúce sa jednotlivca. Dôsledkom toho je, že tá istá informácia sa môže v tom istom čase týkať rôznych jednotlivcov v závislosti od toho, ktorý prvok je vzhľadom na každú túto osobu prítomný. Tá istá informácia sa môže týkať jednotlivca Titia v dôsledku prítomnosti prvku „obsah“ (údaje sú jasne o Titiovi) A Gaia v dôsledku prítomnosti prvku „účel“ (údaje sa budú používať, aby sa s Gaiom zaobchádzalo určitým spôsobom) A Sempronia v dôsledku prítomnosti prvku „výsledok“ (je pravdepodobné, že údaje budú mať dosah na práva a záujmy Sempronia). To zároveň znamená, že nie je nutné, aby boli údaje priamo „zamerané“ na určitú osobu, aby sa považovali za údaje týkajúce sa tejto osoby. V dôsledku predchádzajúcej analýzy je potrebné odpovedať na otázku, či sa údaje týkajú určitej osoby, v prípade každého údajového prvku osobitne. Podobne je pri uplatňovaní hmotnoprávnych ustanovení (napríklad o rozsahu pôsobnosti práva na prístup) potrebné uvedomiť si, že informácie sa môžu týkať rôznych osôb.

Príklad č. 9: Informácie uvedené v zápisnici zo zasadnutia

Príkladom potreby vykonávať predchádzajúcu analýzu každej informácie samostatne sú informácie uvádzané v zápisnici zo zasadnutia, v ktorej sa zvyčajne zaznamenáva

prítomnosť účastníkov Titia, Gaia a Sempronia; vyhlásenia Titia a Gaia; a správa z rokovania o určitých témach, ktorú zhrnul autor zápisnice Sempronius. Za osobné údaje týkajúce sa Titia sa môže považovať iba informácia, že sa zúčastnil zasadnutia v určitom čase a na určitom mieste a že predniesol určité vyhlásenia. Informácie o prítomnosti Gaia na zasadnutí, jeho vyhláseniach a o prerokovaní určitého problému tak, ako ich zhrnul Sempronius, NIE sú osobnými údajmi týkajúcimi sa Titia. Je to tak aj v prípade, že sú tieto informácie uvedené v tom istom dokumente a dokonca aj vtedy, ak to bol Titius kto na zasadnutí nastolil otázku, o ktorej sa rokovalo. Na tieto informácie sa preto nevzťahuje Titiovo právo na prístup k jeho vlastným osobným údajom. To, či sa informácie môžu považovať za osobné údaje Gaia a Sempronia a do akej miery, sa bude musieť stanoviť samostatne pomocou už opísanej analýzy.

3. TRETÍ PRVOK: „IDENTIFIKOVANÁ ALEBO IDENTIFIKOVATEĽNÁ“ [FYZICKÁ OSOBA]

Smernica vyžaduje, aby sa informácie týkali fyzickej osoby, ktorá je „identifikovaná“ alebo „identifikovateľná“. Táto skutočnosť vyvoláva tieto úvahy.

Fyzická osoba sa vo všeobecnosti môže považovať za „identifikovanú“ vtedy, keď je v rámci skupiny osôb „odlíšená“ od všetkých ostatných príslušníkov skupiny. Fyzická osoba je preto „identifikovateľná“ vtedy, keď napriek tomu, že osoba ešte nebola identifikovaná, je možné ju identifikovať (čo je význam prípony „-teľná“). Táto druhá možnosť je preto v praxi hraničnou podmienkou určujúcou, či sú informácie v rámci rozsahu pôsobnosti tretieho prvku.

Identifikácia sa obvykle realizuje prostredníctvom konkrétnych informácií, ktoré môžeme nazvať „identifikátormi“ a ktoré majú osobitne privilegovaný a úzky vzťah ku konkrétnemu jednotlivcovi. Príkladmi sú vonkajšie znaky vzhľadu tejto osoby, napríklad, výška, farba vlasov, oblečenie, atď. … alebo vlastnosti osoby, ktoré sa nedajú okamžite zistiť, napríklad, profesia, funkcia, meno, atď. Smernica uvádza tieto „identifikátory“ v definícii „osobných údajov“ v článku 2, keď uvádza, že fyzická osoba je osoba, ktorú *„možno identifikovať priamo alebo nepriamo, najmä pomocou overenia identifikačného čísla alebo jedného alebo viacerých faktorov špecifických pre jej fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu“*.

„Priamo“ alebo „nepriamo“ identifikovateľná

Ďalšie objasnenie je uvedené v komentári k článkom zmeneného a doplneného návrhu Komisie v tom zmysle, že *„osobu možno identifikovať priamo menom alebo nepriamo telefónnym číslom, evidenčným číslom auta, číslom sociálneho poistenia, číslom cestovného pasu alebo spojením dôležitých kritérií, ktoré umožňujú, aby bola spoznaná zúžením skupiny, do ktorej patrí (vek, povolanie, bydlisko, atď.)“*. Z toho je vidno, že miera, do akej sú určité identifikátory dostačujúce na dosiahnutie identifikácie, závisí od kontextu konkrétnej situácie. Veľmi bežné priezvisko nebude na identifikáciu osoby – t. j. na vyčlenenie niekoho z celej populácie krajiny – dostačujúce, zatiaľ čo je pravdepodobné, že bude dostačujúce na dosiahnutie identifikácie žiaka v triede. Aj doplňujúca informácia, napríklad, „osoba, ktorá má na sebe čierny oblek“, môže určiť niekoho z okoloidúcich čakajúcich pri semafore. Takže otázka, či jednotlivec, ktorého sa informácie týkajú, je identifikovaný alebo nie, závisí od okolností prípadu.

Pokiaľ ide o „priamo“ identifikované alebo identifikovateľné osoby, **meno** osoby je v skutočnosti najbežnejším identifikátorom a v praxi pojem „identifikovaná osoba“ znamená veľmi často odkaz na meno osoby.

Na overenie tejto identity sa musí meno osoby niekedy spojiť s ďalšími informáciami (dátum narodenia, mená rodičov, adresa alebo fotografia tváre), aby sa zabránilo zámene medzi uvedenou osobou a možnými menovcami. Napríklad informáciu, že Titius dlhuje istú sumu peňazí možno považovať za informáciu, ktorá sa týka identifikovaného jednotlivca, pretože je spojená s menom osoby. Meno je informáciou, ktorá prezrádza, že jednotlivec využíva túto kombináciu písmen a hlások na to, aby sa odlíšil od iných osôb a aby ho rozpoznali iné osoby, s ktorými si vytvára vzťahy. Meno môže byť aj východiskom vedúcim k informácii o tom, kde osoba žije alebo kde ju možno nájsť, môže tiež poskytnúť informácie o osobách v jej rodine (prostredníctvom priezviska) a mnohých právnych a sociálnych vzťahoch spojených s uvedeným menom (záznamy o vzdelaní, lekárske záznamy, bankové účty). Dokonca umožňuje spoznať vzhľad osoby, ak sa jej fotografia spája s uvedeným menom. Všetky tieto nové informácie spojené s menom môžu niekomu umožniť zamerať sa na konkrétneho jednotlivca, a preto sa pôvodné informácie prostredníctvom identifikátorov spájajú s fyzickou osobou, ktorú možno odlíšiť od iných jednotlivcov.

Pokiaľ ide o „nepriamo“ identifikované alebo identifikovateľné osoby, táto kategória sa zväčšia týka javu „jedinečných kombinácií“, či už malého alebo veľkého rozmeru. V prípadoch, keď rozsah dostupných identifikátorov nikomu neumožňuje *na prvý pohľad* vyčleniť konkrétnu osobu, uvedená osoba môže byť stále „identifikovateľná“, pretože uvedená informácia v kombinácii s inými informáciami (či už tieto informácie uchoval kontrolór údajov alebo nie) umožní odlíšiť jednotlivca od iných osôb. Práve na túto skutočnosť odkazuje smernica formuláciou o „jednom alebo viacerých faktoroch špecifických pre jej fyzickú, fyziologickú, duševnú, hospodársku, kultúrnu alebo sociálnu identitu“. Niektoré charakteristiky sú tak špecifické, že niekoho možno identifikovať bez akejkoľvek námahy („súčasný premiér Španielska“) avšak aj kombinácia určitých podrobností určitej kategórie (veková kategória, regionálny pôvod atď.) môže byť za určitých okolností takisto smerodajná, najmä ak má osoba prístup k určitému druhu doplňujúcich informácií. Tento jav intenzívne skúmali štatistickí pracovníci, ktorí sa vždy usilujú zabrániť porušeniu dôvernosti údajov.

Príklad č. 10: Neúplné informácie v tlači

Sú uverejnené informácie o niekdajšom trestnom prípade, ktorý v minulosti vyvolal veľký záujem verejnosti. Pri uverejnení v súčasnosti sa neuvádzajú žiadne tradičné identifikátory, najmä žiadne mená, ani dátumy narodenia dotknutých osôb.

Zdá sa, že nie je neprimerane ťažké získať doplňujúce informácie, ktoré umožňujú zistiť hlavné osoby zapojené do prípadu, napríklad, keď si pozrieme noviny z príslušného obdobia. Dá sa predpokladať, že niekto niečo také skutočne urobí (vyhľadá si staré noviny) a veľmi pravdepodobne získa mená a iné identifikátory osôb uvedených v príklade. Preto sa zdá opodstatnené považovať informácie v danom príklade za „informácie o identifikovateľných osobách“ a ako také za „osobné údaje“.

Tu je potrebné uviesť, že hoci sa identifikácia prostredníctvom mena v praxi vyskytuje najbežnejšie, nie je meno na identifikáciu jednotlivca potrebné vo všetkých prípadoch. Napríklad vtedy, ak sa na určenie osoby používajú iné „identifikátory“. Počítačové súbory registrujúce osobné údaje zvyčajne priraďujú zaregistrovaným osobám

jedinečný identifikátor, aby sa zabránilo zámene dvoch osôb v súbore. Pomocou nástrojov sledovania internetovej prevádzky je možné na internete jednoducho zistiť správanie počítača, a teda aj jeho užívateľa. Takto je možné z rôznych prvkov poskladať obraz o osobnosti jednotlivca, aby sa mu prisúdili určité rozhodnutia. Bez toho, aby sa vôbec zisťovalo meno a adresa jednotlivca, je možné zaradiť túto osobu do kategórie na základe socioekonomických, psychologických, filozofických alebo iných kritérií a prisúdiť mu určité rozhodnutia, keďže kontaktné miesto jednotlivca (počítača), ktoré používa, si už nutne nevyžaduje odhalenie jeho identity v úzkom zmysle. Inými slovami, možnosť identifikovať jednotlivca už nutne neznamená schopnosť zistiť jeho meno. Táto skutočnosť sa odráža v definícii osobných údajov[10].

Európsky súdny sa dvor v tomto smere vyjadril, že „*uvedenie odkazov na internetovej stránke na rôzne osoby a ich identifikovanie menami alebo inými prostriedkami, napríklad uvedením ich telefónneho čísla alebo informácií* týkajúcich sa *ich pracovných podmienok a záľub, predstavuje spracovanie osobných údajov [...] v zmysle [...] smernice 95/46/ES*“[11].

Príklad č. 11: Žiadatelia o azyl

Žiadateľom o azyl, ktorí v azylovom zariadení zatajujú svoje skutočné mená, boli pridelené na administratívne účely kódové čísla. Takéto číslo slúži ako identifikátor, ku ktorému sa potom priraďujú rôzne informácie týkajúce sa pobytu žiadateľa o azyl v inštitúcii a prostredníctvom fotografie alebo iných biometrických ukazovateľov je kódové číslo úzko a bezprostredne prepojené s fyzickou osobou, čo umožňuje jej odlíšenie od iných žiadateľov o azyl a priradenie rôznych informácií, ktoré sa potom týkajú iba „identifikovanej“ fyzickej osoby.

Článok 8 ods. 7 tiež stanovuje, že „členské štáty stanovia podmienky, za ktorých bude možné spracovávať štátne identifikačné číslo alebo akýkoľvek iný identifikačný znak všeobecného uplatnenia“. Toto ustanovenie neobsahuje žiadny konkrétny náznak, aký druh podmienok by mali členské štáty prijať, je však uvedené v článku, ktorý sa zaoberá citlivými údajmi. Odôvodnenie 33 sa odvoláva na tento druh údajov ako na *„údaje, ktoré sú vzhľadom na svoj charakter schopné zasahovať do základných slobôd alebo súkromia“*. Je opodstatnené domnievať sa, že zákonodarca pravdepodobne pociťoval podobné obavy týkajúce sa vnútroštátnych identifikačných čísiel v dôsledku ich silného potenciálu ľahko a jednoznačne priradiť rôzne informácie k určitému jednotlivcovi.

Prostriedky na identifikáciu

V odôvodnení 26 smernice sa osobitná pozornosť venuje pojmu „identifikovateľný“, keď sa v ňom uvádza, že *„keďže k určeniu, či je osoba identifikovateľná, by sa mali vziať do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby.“* To znamená, že iba hypotetická možnosť určiť jednotlivca nie je dostatočná na to, aby sa osoba považovala za „identifikovateľnú“. Ak po zohľadnení „*všetkých prostriedkov, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba“*, uvedená možnosť neexistuje alebo je zanedbateľná, osoba by sa nemala pokladať za

[10] Správa o uplatňovaní zásad ochrany údajov na celosvetové telekomunikačné siete pána Yves POULLETA a jeho tímu pre výbor T-PD Rady Európy, bod 2.3.1, T-PD (2004) 04, v konečnom znení.

[11] Rozsudok Európskeho súdneho dvora C-101/2001 zo 6.11.2003 (Lindqvist), §27.

„identifikovateľnú“ a ani informácie za „osobné údaje“. V kritériu *„všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba“* by sa mali zohľadniť všetky príslušné faktory. Náklady na vykonanie identifikácie sú jedným, ale nie jediným faktorom. Mal by sa zohľadniť zamýšľaný účel, štruktúra spracovanie, výhody očakávané kontrolórom, záujmy jednotlivcov, ako aj riziko organizačných dysfunkcií (napríklad porušenia povinnosti zachovávať dôvernosť informácií) a technické nedostatky. Na druhej strane je tento test dynamický a mal by zohľadniť súčasný stav technológie v čase spracovania a možnosti rozvoja v období, počas ktorého sa budú údaje spracovávať. Je možné, že so všetkými dnešnými prostriedkami, u ktorých je primeraná pravdepodobnosť využitia, nie je v súčasnosti identifikácia realizovateľná. Ak sa údaje majú uchovať jeden mesiac, pravdepodobne sa neočakáva, že identifikácia bude možná počas „životnosti“ informácií a informácie by sa nemali považovať za osobné údaje. Ak sa však majú uchovávať 10 rokov, kontrolór by mal posúdiť možnosť identifikácie, ktorá môže nastať napríklad v deviatom roku ich životnosti a ktorá z nich môže urobiť v uvedenej dobe osobné údaje. Systém by mal byť schopný prispôsobiť sa tomuto vývoju, ktorý môže nastať, a v pravý čas aplikovať vhodné technické a organizačné opatrenia.

Príklad č. 12: Zverejnenie röntgenových snímok spolu s pacientovým krstným menom

Veľmi nezvyčajná röntgenová snímka jednej ženy bola uverejnená vo vedeckom časopise spolu s jej krstným menom. Krstné meno osoby spolu s vedomosťou jej príbuzných a známych, že trpí určitou chorobou, činia túto osobu identifikovateľnou mnohým osobám a röntgenová snímka by sa potom mala pokladať za osobný údaj.

Príklad č. 13: Údaje z farmaceutického výskumu

Nemocnice alebo jednotliví lekári zasielajú údaje z lekárskych záznamov o svojich pacientoch nejakej spoločnosti na účely lekárskeho výskumu. Mená pacientov sa nepoužívajú, používajú sa iba sériové čísla náhodne priradené každému klinickému prípadu, aby sa zabezpečila súvislosť a aby sa zabránilo zámene s informáciami o iných pacientoch. Mená pacientov poznajú iba príslušní lekári, ktorí sú viazaní povinnosťou zachovávať lekárske tajomstvo. Údaje neobsahujú žiadne doplňujúce informácie, ktoré by umožnili identifikáciu pacientov kombináciou týchto informácií. Okrem toho boli prijaté všetky ďalšie opatrenia, ktoré zabraňujú tomu, aby boli údajové subjekty identifikované alebo sa stali identifikovateľnými, či už ide o právne, technické alebo organizačné opatrenia. Za týchto okolností môže orgán na ochranu údajov usúdiť, že pri spracovávaní údajov farmaceutickou spoločnosťou neexistujú žiadne prostriedky, v prípade ktorých existuje primeraná pravdepodobnosť využitia na identifikáciu údajových subjektov.

Jedným z už uvedených dôležitých faktorov posúdenia *„všetkých prostriedkov, u ktorých je primeraná pravdepodobnosť, že sa využijú“* na identifikáciu osôb, je účel, ktorý pri spracovaní údajov sleduje kontrolór údajov. Vnútroštátne orgány na ochranu údajov riešili prípady, v ktorých na jednej strane kontrolór tvrdí, že sa spracúvajú iba jednotlivé informácie bez odkazu na meno alebo akékoľvek iné priame identifikátory a zastáva názor, že tieto údaje by sa nemali považovať za osobné údaje a nemali by podliehať pravidlám o ochrane údajov. Spracovanie uvedených informácií má na druhej strane zmysel iba vtedy, ak umožňujú identifikáciu špecifických jednotlivcov a zaobchádzanie s nimi určitým spôsobom. V týchto prípadoch, keď účel spracovania v sebe zahŕňa identifikáciu jednotlivcov, možno predpokladať, že kontrolór alebo akákoľvek iná príslušná osoba má alebo bude mať prostriedky, u ktorých je „primeraná

pravdepodobnosť, že sa využijú“ na identifikáciu údajových subjektov. Tvrdenie, že jednotlivci nie sú identifikovateľní v prípade, keď je účelom spracovania práve ich identifikácia, by bolo jasným rozporom. Informácie by sa preto mali považovať za informácie, ktoré sa týkajú identifikovateľných osôb a spracovanie by malo podliehať pravidlám o ochrane údajov.

Príklad č. 14: Videomonitorovanie

Táto otázka má osobitný význam, pokiaľ ide o videomonitorovanie, v prípade ktorého kontrolóri údajov často tvrdia, že identifikácia by sa uskutočnila iba v malom percente zhromaždeného materiálu, a preto sa predtým, ako sa naozaj uskutoční identifikácia v týchto niekoľkých prípadoch, nespracúvajú žiadne osobné údaje. Keďže však účelom videomonitorovania je identifikácia osôb, ktoré vidno na videozáznamoch vo všetkých prípadoch, v ktorých kontrolór považuje takúto identifikáciu za nutnú, celé uplatňovanie ako také sa musí pokladať za spracovanie údajov o identifikovateľných osobách aj vtedy, keď nie sú niektoré osoby nahrané na videozázname v praxi identifikovateľné.

Príklad č. 15: Dynamické IP adresy

Pracovná skupina považuje IP adresy za údaje týkajúce sa identifikovateľnej osoby. Uviedla, že *„poskytovatelia prístupu na internet a správcovia miestnych sietí môžu pomocou primeraných prostriedkov identifikovať užívateľov internetu, ktorým pridelili IP adresy pretože zvyčajne systematicky „zaznamenávajú“ do súboru dátum, čas, trvanie a dynamickú IP adresu pridelenú užívateľovi internetu. To isté možno povedať o poskytovateľoch internetových služieb, ktorí vedú prevádzkový denník na serveri HTTP. V týchto prípadoch možno nepochybne hovoriť o osobných údajoch v zmysle článku 2 písm. a) smernice ...)“*[12]

Najmä v prípadoch, keď sa IP adresy spracúvajú na účely identifikácie užívateľov počítača (napríklad vlastníkmi autorských práv, ktorí chcú stíhať užívateľov počítača za porušenie práv duševného vlastníctva) kontrolór očakáva, že budú k dispozícii „prostriedky, u ktorých je primeraná pravdepodobnosť, že sa využijú“ na identifikáciu osôb, napríklad prostredníctvom súdov, na ktoré sa obrátia (inak nemá zhromažďovanie informácií žiadny význam), a preto by sa informácie mali považovať za osobné údaje.

Osobitným prípadom by boli určité druhy IP adries, ktoré za určitých okolností skutočne neumožňujú identifikáciu užívateľa z rôznych technických a organizačných dôvodov. Jedným z príkladov by mohli byť IP adresy pridelené počítaču v internetovej kaviarni, kde sa nevyžaduje žiadna identifikácia zákazníkov. Mohlo by sa namietať, že údaje zhromaždené o využívaní počítača X počas určitého časového rámca neumožňujú identifikáciu užívateľa primeranými prostriedkami, a preto nie sú osobnými údajmi. Je však nutné uviesť, že poskytovatelia internetových služieb pravdepodobne nebudú vedieť, či príslušná IP adresa je alebo nie je adresou, ktorá umožňuje identifikáciu, a že spracujú údaje spojené s touto IP adresou rovnakým spôsobom, ako spracúvajú informácie spojené s IP adresami užívateľov, ktorí sú riadne zaregistrovaní a identifikovateľní. Takže pokiaľ poskytovateľ internetových služieb

[12] WP 37: Súkromie na internete – Integrovaný prístup EÚ k on-line ochrane údajov – prijaté 21.11.2000.

nemôže s absolútnou istotou rozlíšiť, či údaje zodpovedajú užívateľom, ktorí sa nedajú identifikovať, bude musieť pre istotu spracovať všetky informácie IP ako osobné údaje.

Príklad č. 16: Škoda spôsobená graffiti

Vozidlá na prepravu osôb vlastnené dopravnou spoločnosťou sú opakovane poškodzované graffiti. Aby sa stanovila škoda a aby sa uľahčilo vymáhanie právnych nárokov voči ich autorom, spoločnosť vedie register obsahujúci informácie o okolnostiach škôd, ako aj fotografie poškodených vecí a „značiek“ alebo „podpisu“ autora. Vo chvíli zaevidovania informácie do registra nie sú pôvodcovia škody známi, ani nie je známe, komu „podpis“ patrí. Je možné, že nebudú nikdy známi. Účelom spracovania je však presné určenie jednotlivcov, ktorých sa informácie ako pôvodcov škody týkajú, aby sa mohla od nich vymáhať zákonná náhrada škody. Takéto spracovanie má zmysel, ak kontrolór údajov očakáva, že je „primerane pravdepodobné“, že jedného dňa budú existovať prostriedky na identifikovanie jednotlivca. Informácie obsiahnuté na fotografiách by sa mali považovať za informácie týkajúce sa „identifikovateľných“ jednotlivcov, informácie v registri za „osobné údaje“ a spracovanie by malo podliehať pravidlám o ochrane údajov, ktoré umožňujú takéto spracovanie ako zákonné za určitých okolností a pri poskytnutí určitých záruk.

V prípade, že identifikácia údajového subjektu nie je zahrnutá do účelu spracovania, majú veľmi dôležitú úlohu technické opatrenia zabraňujúce identifikácii. Zavedenie vhodných najmodernejších technických a organizačných opatrení na ochranu údajov pred identifikáciou môže ovplyvniť posúdenie, či osoby nie sú identifikovateľné, zohľadňujúc *všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba* na identifikáciu jednotlivcov. V tomto prípade nie je uskutočnenie uvedených opatrení *dôsledkom* právnej povinnosti vyplývajúcej z článku 17 smernice (ktorý sa uplatňuje iba vtedy, ak sú informácie predovšetkým osobnými údajmi), ale skôr *podmienkou,* aby sa informácie nepokladali za osobné údaje a ich spracovanie nepodliehalo smernici.

Pseudonymizované údaje

Pseudonymizácia je proces maskovania identít. Cieľom tohto procesu je byť schopný zhromaždiť doplňujúce údaje týkajúce sa toho istého jednotlivca bez nutnosti poznať jeho totožnosť. Má osobitný význam v rámci výskumu a štatistiky.

Pseudonymizácia sa môže uskutočniť vysledovateľným spôsobom pomocou zoznamov súladu identít a ich pseudonymov alebo pomocou dvojsmerných kryptografických algoritmov na pseudonymizáciu. Identity sa môžu zamaskovať aj spôsobom neumožňujúcim opätovnú identifikáciu, napríklad jednosmernou kryptografiou, pri ktorej sa vo všeobecnosti vytvárajú anonymizované údaje.

Efektívnosť postupu pseudonymizácie závisí od niekoľkých faktorov (v ktorom štádiu sa postup používa, ako je zabezpečený proti spätnému vysledovaniu, veľkosť populácie, v ktorej je jednotlivec utajený, schopnosti spojiť jednotlivé transakcie alebo záznamy s tou istou osobou atď.). Pseudonymy by mali byť náhodné a nepredvídateľné. Počet možných pseudonymov by mal byť tak veľký, aby sa ten istý pseudonym nikdy nevybral náhodne dvakrát. Ak sa vyžaduje vysoký stupeň bezpečnosti, súbor potenciálnych

pseudonymov musí byť aspoň rovný rozsahu hodnôt bezpečných kryptografických hašovacích funkcií[13].

Vysledovateľne pseudonymizované údaje sa môžu považovať za informácie o jednotlivcoch, ktorí sú *nepriamo identifikovateľní*. Používanie pseudonymu v skutočnosti znamená, že je možné spätne vysledovať jednotlivca, takže jeho totožnosť sa dá zistiť avšak iba za vopred definovaných okolností. V takom prípade, aj keď sa uplatňujú pravidlá o ochrane údajov, budú príslušné riziká pre jednotlivcov, pokiaľ ide o spracovanie takýchto nepriamo identifikovateľných informácií, veľmi často nízke, takže uplatňovanie týchto pravidiel bude opodstatnene flexibilnejšie, ako keby sa spracovali informácie o priamo identifikovateľných jednotlivcov.

Kľúčom kódované údaje

Kľúčom kódované údaje sú klasickým príkladom pseudonymizácie. Informácie sa týkajú jednotlivcov, ktorí sú označení kódom, zatiaľ čo kľúč, ktorý vytvára zhodu medzi kódom a spoločnými identifikátormi jednotlivcov (napríklad menom, dátumom narodenia, adresou) sa uchováva oddelene.

Príklad č. 17: Nesúhrnné údaje pre štatistiky

Príkladom poukazujúcim na dôležitosť zohľadnenia všetkých okolností pri posudzovaní, či je v prípade prostriedkov na identifikáciu „primeraná pravdepodobnosť“, že ich nejaká osoba využije, by mohli byť osobné údaje spracovávané vnútroštátnym štatistickým ústavom, kde sa informácie v určitom štádiu uchovávajú v nesúhrnnej forme a týkajú sa špecifických jednotlivcov; namiesto mena je im pridelený kód (napríklad jednotlivec označený kódom X1234 pije pohár vína viac ako trikrát týždenne). Štatistický ústav uchováva kľúč k týmto kódom (zoznam, v ktorom sa spájajú kódy s menami osôb) oddelene. Uvedený kľúč sa môže považovať za kľúč, u ktorého je „primeraná pravdepodobnosť, že ho využije“ štatistický ústav, a preto možno súbor informácií týkajúcich sa jednotlivca považovať za osobné údaje a mal by podliehať pravidlám ústavu o ochrane údajov. Môžeme si predstaviť príklad, že zoznam s údajmi o požívaní alkoholu spotrebiteľmi sa zašle vnútroštátnemu výrobcovi vína s cieľom umožniť mu podporiť jeho verejné stanovisko štatistickými údajmi. Na určenie, či uvedený zoznam informácií predstavuje osobné údaje, je potrebné zhodnotiť, či je možné identifikovať jednotlivých konzumentov vína pri *„zohľadnení všetkých prostriedkov, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba“*.

Ak sa pre každú špecifickú osobu použije osobitný kód, riziko identifikácie nastáva vždy, keď je možné získať prístup ku kľúču, ktorý sa používa na zakódovanie. Riziká vniknutia zvonku, pravdepodobnosť, že by niekto v rámci zasielajúcej organizácie – napriek jeho povinnosti zachovávať služobné tajomstvo – poskytol kľúč *a* uskutočniteľnosť nepriamej identifikácie sú faktory, ktoré je potrebné zohľadniť pri určovaní, či osoby môžu byť identifikované pri *zohľadnení všetkých prostriedkov, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba*, a teda pri určovaní či by sa informácie mali považovať za „osobné údaje“. Ak áno, budú sa uplatňovať pravidlá o ochrane údajov. Uvedené pravidlá o ochrane údajov

[13] Pozri pracovný dokument „Technológie na posilnenie ochrany súkromia“ pracovnej skupiny pre „technológie na posilnenie ochrany súkromia“ výboru pre „technické a organizačné aspekty ochrany údajov“ nemeckých federálnych a štátnych komisárov pre ochranu údajov (október 1997), uverejnený na internetovej adrese http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

by mohli zohľadňovať, či sú riziká pre jednotlivcov znížené, a podrobiť spracovanie údajov viac alebo menej prísnym podmienkam na základe flexibility, ktorú umožňujú pravidlá smernice.

Ak naopak každá osoba nemá osobitný kód, ale na označenie jednotlivcov v rôznych mestách a údajov z rôznych rokov (rozlišuje sa len konkrétny jednotlivec v rámci roka a v rámci vzorky v tom istom meste) sa používa rovnaké kódové číslo (napr. „123“), kontrolór alebo tretia strana by mohli identifikovať špecifického jednotlivca iba vtedy, ak by vedeli ktorého roku a ktorého mesta sa údaje týkajú. Ak sa tieto doplňujúce informácie stratili a neexistuje primeraná pravdepodobnosť, že sa opäť získajú, bolo by možné domnievať sa, že informácie sa netýkajú identifikovateľných jednotlivcov a nepodliehali by pravidlám o ochrane údajov.

Tento druh údajov sa zvyčajne používa pri klinických pokusoch s liekmi. Smernica 2001/20 zo 4. apríla 2001 o uplatňovaní dobrej klinickej praxe a výkone klinických pokusov[14] stanovuje právny rámec na vykonávanie týchto činností. Lekár/výskumný pracovník („výskumník“) testujúci lieky zhromažďuje informácie o klinických výsledkoch o každom pacientovi, pričom mu pridelí kód. Výskumný pracovník poskytuje informácie farmaceutickej spoločnosti alebo iným príslušným stranám („sponzorom“) iba v tejto zakódovanej forme, pretože sa zaujímajú iba o biologicko-štatistické informácie. Výskumník však oddelene uchováva kľúč, ktorý spája tento kód s bežnými informáciami umožňujúcimi identifikáciu pacientov. Aby sa chránilo zdravie pacientov v prípade, že sa ukáže, že lieky predstavujú nebezpečenstvo, výskumník je povinný uchovávať tento kľúč, aby bolo možné jednotlivých pacientov v prípade potreby identifikovať a poskytnúť im primeranú liečbu.

Otázkou je v tomto prípade, či sa údaje použité na klinické pokusy môžu považovať za údaje týkajúce sa „identifikovateľných“ fyzických osôb, a teda za údaje podliehajúce pravidlám o ochrane údajov. Podľa už opísanej analýzy by sa pri určovaní, či je osoba identifikovateľná, mali zohľadniť všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich použije buď kontrolór alebo ľubovoľná iná osoba na identifikáciu uvedenej osoby. V tomto prípade je identifikácia jednotlivcov (aby sa v prípade potreby použila vhodná liečba) jedným z účelov spracovania údajov kódovaných kľúčom. Farmaceutická spoločnosť poskytla prostriedky na spracovanie, podnikla také organizačné opatrenia a nadviazala s výskumným pracovníkom, ktorý má kľúč, také vzťahy, aby identifikácia jednotlivcov nebola iba niečím, čo sa *môže* stať, ale skôr niečím, čo sa za určitých okolností *musí* stať. Identifikácia pacientov je takto zakotvená v účeloch a prostriedkoch spracovania. V tomto prípade možno dospieť k záveru, že takéto údaje kódované kľúčom predstavujú pre všetky strany, ktoré by mohli byť zapojené do možnej identifikácie, informácie týkajúce sa identifikovateľných fyzických osôb a mali by podliehať pravidlám právnych predpisov o ochrane údajov. To však neznamená, že akýkoľvek iný kontrolór údajov, ktorý spracúva ten istý súbor zakódovaných údajov by spracovával osobné údaje, ak je v rámci osobitného systému, v ktorom títo iní kontrolóri pracujú, jednoznačne vylúčená opätovná identifikácia, a ak boli z tohto hľadiska prijaté primerané technické opatrenia.

V iných oblastiach výskumu alebo rovnakého projektu sa pri vytváraní protokolov a postupu mohla opätovná identifikácia subjektu údajov vylúčiť, napríklad pretože neexistujú žiadne terapeutické aspekty. Z technických alebo iných dôvodov môže stále

[14] Ú. v. ES L 121, 1.5.2001, s. 34.

existovať spôsob, ako zistiť, ku ktorým osobám patria konkrétne klinické údaje, ale nepredpokladá sa ani sa neočakáva, že za nejakých okolností dôjde k identifikácii, a zaviedli sa primerané technické opatrenia (napríklad kryptografické, nevratné hašovanie), ktoré majú zabrániť, aby k tomu došlo. V tomto prípade, aj keď môže dôjsť k identifikácii údajových subjektov napriek všetkým týmto protokolom a opatreniam (v dôsledku nepredvídateľných okolností, medzi ktoré patrí náhodná zhoda vlastností údajového subjektu, ktorými sa odhalí jeho totožnosť), informácie spracované pôvodným kontrolórom sa nesmú považovať za informácie týkajúce sa identifikovaných alebo identifikovateľných jednotlivcov, zohľadňujúc *všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba*. Ich spracovanie teda nesmie podliehať ustanoveniam smernice. Odlišným prípadom je, keď nový kontrolór účinne získal prístup k identifikovateľným informáciám, ktoré sa v tomto prípade budú nepochybne pokladať za „osobné údaje“.

Často kladené otázky (FAQ 14- otázka a odpoveď č. 7) k systému bezpečný prístav

Otázka kľúčom kódovaných údajov pri farmaceutickom výskume bola riešená v rámci systému bezpečný prístav[15]. FAQ 14- otázka a odpoveď č.7 znie takto:

FAQ 14 – Farmaceutické a lekárske výrobky

7. *Otázka: Výskumné údaje hlavný vedúci pracovník výskumu vždy zakóduje v ich pôvodnom stave osobitným kľúčom, aby sa neodhalila totožnosť jednotlivých osôb, ktoré sú predmetom údajov. Farmaceutickým spoločnostiam sponzorujúcim takýto výskum sa tento kľúč neposkytuje. Tento osobitný kľúčový kód vlastní len spomínaný výskumný pracovník, aby mohol/mohla za určitých okolností identifikovať osobu, ktorá je predmetom výskumu (napríklad v prípade, že je potrebná následná lekárska starostlivosť). Predstavuje prenos takýmto spôsobom zakódovaných údajov z EÚ do Spojených štátov prenos osobných údajov podliehajúcich zásadám bezpečného prístavu?*

7. Odpoveď: Nie. Takýto prenos nepredstavuje prenos osobných údajov, ktoré by podliehali zásadám.

Pracovná skupina sa domnieva, že toto vyhlásenie v systéme bezpečného prístavu je zlučiteľné s už vysvetleným odôvodnením, aby sa takéto informácie považovali za osobné údaje podliehajúce smernici. Táto FAQ nie je v skutočnosti dostatočne presná, pretože sa v nej neuvádza, komu a za akých podmienok sa údaje zasielajú. Pracovná skupina sa domnieva, že FAQ sa týka prípadu, keď sa údaje kódované kľúčom zasielajú príjemcovi v USA (napríklad farmaceutickej spoločnosti), ktorý dostáva iba údaje kódované kľúčom a nikdy sa nedozvie totožnosť pacientov, ktorá je známa a bude známa v prípade potreby liečby iba lekárskemu odborníkovi/výskumnému pracovníkovi v EÚ, ale nikdy spoločnosti v USA.

Anonymné údaje

„Anonymné údaje“ v zmysle smernice sa môžu definovať ako akékoľvek informácie týkajúce sa fyzickej osoby v prípade, že túto osobu nemôže, či už kontrolór údajov alebo akákoľvek iná osoba, identifikovať, *berúc do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba* na

[15] Rozhodnutie Komisie 2000/520/ES z 26.7.2000 – Ú. v. ES L 215/7 z 25.8.2000.

identifikáciu uvedeného jednotlivca. „Anonymizované údaje“ by preto boli anonymnými údajmi, ktoré sa predtým týkali identifikovateľnej osoby, ale v prípade ktorých už nie je táto identifikácia viac možná. Odôvodnenie 26 sa tiež odvoláva na tento pojem, keď sa v ňom uvádza, že *„zásady ochrany sa nebudú vzťahovať na údaje poskytnuté anonymne, a to tak, že predmet údajov sa už nebude dať identifikovať“*. Posúdenie, či údaje umožňujú alebo neumožňujú identifikáciu jednotlivca a či informácie možno alebo nemožno považovať za anonymné opäť závisí od okolností a mala by sa vykonať analýza od prípadu k prípadu s osobitným odkazom na mieru, do akej je primerane pravdepodobné, že prostriedky sa použijú na identifikáciu, ako je uvedené v odôvodnení 26. To je osobitne dôležité v prípade štatistických informácií, kde napriek skutočnosti, že informácie sa môžu predložiť ako súhrnné údaje, nie je pôvodná vzorka dostatočne veľká a ďalšie informácie môžu umožniť identifikáciu jednotlivcov.

Príklad č. 18: Štatistické prieskumy a kombinácia jednotlivých informácií

Štatistickí pracovníci okrem svojej všeobecnej povinnosti dodržiavať pravidlá ochrany údajov, aby sa zabezpečila anonymita štatistických prieskumov, podliehajú osobitnej povinnosti zachovávať služobné tajomstvo a na základe uvedených pravidiel majú zakázané uverejňovať neanonymné údaje. To ich zaväzuje uverejňovať súhrnné štatistické údaje, ktoré sa v žiadnom prípade nedajú priradiť identifikovanej osobe, ktorá je súčasťou štatistického údaju. Toto pravidlo je osobitne dôležité v prípade uverejňovania údajov o sčítaní obyvateľstva. V každej situácii by sa mala stanoviť hranica, pod ktorou sa považuje za možné identifikovať príslušné osoby. Ak sa ukáže, že niektoré kritérium vedie k identifikácii v danej kategórii osôb, nech je akokoľvek veľká (t. j. iba jeden lekár operuje v meste so 6000 obyvateľmi), toto „diskriminačné“ kritérium by sa malo zrušiť celkom alebo by sa mali pridať ďalšie kritériá, aby sa „rozriedili“ výsledky o danej osobe a tak sa zachovalo štatistické tajomstvo.

Príklad č. 19: Uverejnenie videomonitorovania

Vlastník obchodu nainštaluje do svojho obchodu kamerový monitorovací systém. Vo svojom obchode zverejní fotografie zlodejov, ktorí boli prichytení pomocou kamerového monitorovacieho systému. Po zásahu polície vymaže tváre zlodejov tak, že ich zatmaví. Po tomto zásahu však stále existuje možnosť, že osoby na fotkách môžu spoznať ich priatelia, príbuzní alebo susedia, pretože sa ešte stále dajú rozpoznať, napríklad podľa postavy, účesu alebo šiat.

4. ŠTVRTÝ PRVOK: „FYZICKÁ OSOBA“

Ochrana, ktorú poskytujú pravidlá smernice, sa vzťahuje na fyzické osoby, teda ľudí. Právo na ochranu osobných údajov je v uvedenom zmysle univerzálnym právom, ktoré sa neobmedzuje na štátnych príslušníkov alebo obyvateľov určitej krajiny. V odôvodnení 2 smernice sa výslovne uvádza, že *„systémy spracovania údajov sú určené na to, aby slúžili človeku“* a že *„musia, nech je akákoľvek štátna príslušnosť fyzických osôb a ich bydlisko, rešpektovať ich základné práva a slobody“*.

Pojem fyzickej osoby je vysvetlený v článku 6 Všeobecnej deklarácie ľudských práv, podľa ktorej *„každý má právo, aby bola všade uznávaná jeho právna osobnosť“*. Pojem osobnosť človeka, pod ktorou sa rozumie schopnosť byť subjektom právnych vzťahov od narodenia jednotlivca až po jeho smrť, je presnejšie vymedzený v právnych predpisoch členských štátov, zvyčajne z oblasti občianskeho práva. Osobné údaje sú preto údajmi, ktoré sa týkajú spravidla identifikovaných alebo identifikovateľných

žijúcich jednotlivcov. Na účely tejto analýzy sa v tejto súvislosti vynára množstvo otázok.

Údaje o zosnulých osobách

Zosnulé osoby nie sú podľa občianskeho práva už fyzickými osobami, a preto sa údaje týkajúce sa zosnulých spravidla nemajú považovať za osobné údaje podliehajúce pravidlám smernice. Údaje o zosnulých však možno v určitých prípadoch stále nepriamo chrániť.

Kontrolór údajov nemusí na druhej strane byť schopný zistiť, či osoba, ktorej sa údaje týkajú, je stále naživе alebo je mŕtva. Ale aj v prípade, že to zistiť dokáže , môžu byť informácie o zosnulých bez rozlíšenia spracované podľa rovnakého režimu, ako informácie o žijúcich osobách. Keďže kontrolór údajov musí plniť povinnosti súvisiace s ochranou údajov, ktoré mu ukladá smernica, pokiaľ ide o údaje o žijúcich osobách, bude pre neho v praxi pravdepodobne ľahšie spracovať aj údaje o zosnulých tak, ako nariaďujú pravidlá o ochrane údajov, než obidva súbory údajov oddeľovať.

Informácie o zosnulých jednotlivcoch sa na druhej strane môžu týkať aj žijúcich osôb. Napríklad, informácia, že zosnulá Gaia trpela hemofíliou naznačuje, že jej syn trpí rovnakou chorobou, pretože táto choroba sa spája s génom obsiahnutým v chromozóme X. Takže v prípade, že sa informácie, ktoré sú údajmi o zosnulom, môžu súčasne považovať za informácie týkajúce sa žijúcej osoby a osobné údaje podliehajúce smernici, potom sa na osobné údaje o zosnulom môžu nepriamo uplatňovať pravidlá o ochrane údajov.

Po tretie, informácie o zosnulých osobách môžu podliehať osobitnej ochrane, ktorú poskytujú iné súbory pravidiel ako právne predpisy o ochrane údajov, ktoré stanovujú hranice toho, čo niektorí nazývajú „*personalitas praeterita*“. Povinnosť zdravotníckych pracovníkov zachovávať lekárske tajomstvo nezaniká smrťou pacienta. Vnútroštátne právne predpisy o práve na osobnú povesť a česť môžu poskytovať ochranu aj pamiatke zosnulého.

A po štvrté, členským štátom nič nebráni, aby rozšírili rozsah pôsobnosti vnútroštátnych právnych predpisov, ktorými sa vykonávajú ustanovenia smernice 95/46/ES, na oblasti, ktoré nie sú zahrnuté do rozsahu jej pôsobnosti za predpokladu, že to nevylučuje žiadne iné ustanovenie právnych predpisov Spoločenstva, ako upozornil Európsky súdny dvor[16]. Je možné, že niektorý vnútroštátny zákonodarca sa môže rozhodnúť rozšíriť ustanovenia vnútroštátnych právnych predpisov o ochrane údajov na niektoré aspekty týkajúce sa spracovania údajov o zosnulých osobách v prípade, že je to odôvodnené oprávnených záujmom[17].

Nenarodené deti

Rozsah, v akom sa pravidlá o ochrane údajov môžu uplatňovať pred narodením dieťaťa, závisí od všeobecného stanoviska vnútroštátnych právnych systémov k ochrane nenarodených detí. S cieľom zohľadniť najmä dedičské práva, niektoré členské štáty uznávajú zásadu, že počaté, ale ešte nenarodené deti sa pokladajú za

---

16 Rozsudok Európskeho súdneho dvora C-101/2001 zo 6.11.2003 (Lindqvist), § 98.

17 Zápisnica zo zasadnutia Rady Európskej únie, 8.2.1995, dokument 4730/95: k článku 2 písm. a) „*Rada a Komisia potvrdzujú, že je na členských štátoch stanoviť, či sa táto smernica má vzťahovať na zosnulé osoby a v akom rozsahu.*“

narodené deti, pokiaľ ide o výhody (a teda môžu získať dedičstvo alebo prijať dar), pod podmienkou, že sa skutočne narodia. V iných členských štátoch sa osobitná ochrana poskytuje osobitnými právnymi ustanoveniami, ktoré tiež podliehajú rovnakej podmienke. Aby bolo možné určiť, či vnútroštátne ustanovenia o ochrane údajov chránia aj informácie o nenarodených deťoch, mal by sa zvážiť uvedený všeobecný prístup vnútroštátneho právneho systému spolu s myšlienkou, že účelom pravidiel o ochrane údajov je chrániť jednotlivca.

Ďalšia otázka súvisí s úvahou, že všeobecná reakcia právneho systému vychádza z predpokladu, že postavenie nenarodených detí je časovo ohraničené tehotenstvom. Nezohľadňuje skutočnosť, že táto situácia môže v skutočnosti trvať podstatne dlhšie, ako je to v prípade zmrazených embryí. Osobitné právne reakcie zaoberajúce sa využitím lekárskych a genetických informácií o embryách možno nájsť v osobitných ustanoveniach o reprodukčných technikách.

Právnické osoby

Keďže definícia osobných údajov sa vzťahuje na jednotlivcov, t. j. fyzické osoby, na informácie týkajúce právnických osôb sa smernica spravidla nevzťahuje a ochrana, ktorú smernica poskytuje, sa na ne neuplatňuje[18]. Určité pravidlá o ochrane údajov sa však za niektorých okolností môžu nepriamo vzťahovať na informácie týkajúce sa podnikateľských subjektov alebo právnických osôb.

Určité ustanovenia smernice 2002/58/ES o súkromí v oblasti elektronických komunikácií sa uplatňujú aj na právnické osoby. Článok 1 tejto smernice stanovuje, že „*2. Ustanovenia tejto smernice spodrobňujú a dopĺňajú smernicu 95/46/ES na účely uvedené v odseku 1. Okrem toho poskytujú ochranu legitímnych záujmov účastníkov, ktorí sú právnickými osobami.*“ Článkami 12 a 13 sa preto rozširuje uplatňovanie určitých ustanovení týkajúcich sa telefónnych zoznamov účastníkov a nevyžiadaných správ aj na právnické osoby.

Informácie o právnických osobách sa môžu na základe ich vecného obsahu tiež pokladať za informácie „týkajúce sa“ fyzických osôb v súlade s kritériami stanovenými v tomto dokumente. Napríklad, ak sa meno právnickej osoby odvodzuje od mena fyzickej osoby. Ďalším príkladom môže byť podniková elektronická pošta, ktorú zvyčajne využíva určitý zamestnanec, alebo informácie o malom podniku (právnicky povedané skôr „objekte“ ako právnickej osobe), v ktorých môže byť opísané správanie jeho vlastníka. Vo všetkých týchto prípadoch, ak kritériá „obsahu“, „účelu“ alebo „výsledku“ umožňujú, aby sa informácie o právnickej osobe alebo o podniku považovali za informácie „týkajúce sa“ fyzickej osoby, mali by sa tieto informácie pokladať za osobné údaje a mali by sa na ne uplatňovať pravidlá o ochrane údajov.

Európsky súdny dvor objasnil, že nič nebráni členským štátom, aby rozšírili rozsah pôsobnosti vnútroštátnych právnych predpisov, ktorými sa vykonávajú ustanovenia smernice, na oblasti, ktoré nie sú zahrnuté do jej rozsahu pôsobnosti za predpokladu, že to nevylučuje žiadne iné ustanovenie právnych predpisov Spoločenstva[19]. Niektoré členské štáty, napríklad Taliansko, Rakúsko alebo Luxembursko, preto rozšírili uplatňovanie určitých ustanovení vnútroštátnych právnych predpisov prijatých podľa

[18] Odôvodnenie 24 smernice: „*keďže právne predpisy týkajúce sa ochrany právnických osôb vo vzťahu k spracovaniu dát, ktoré sa ich týkajú, nie sú ovplyvnené touto smernicou*;“.

[19] Rozsudok Európskeho súdneho dvora C-101/2001 zo 6.11.2003 (Lindqvist), § 98.

smernice (medzi ne patria ustanovenia o bezpečnostných opatreniach) na spracovanie údajov o právnických osobách.

Tak ako v prípade informácií o zosnulých, môžu praktické opatrenia kontrolóra viesť aj k tomu, že údaje o právnickej osobe budú de facto podliehať pravidlám o ochrane údajov. Ak kontrolór údajov zhromažďuje údaje o fyzických a právnických osobách nejasne a zaraďuje ich do tých istých súborov údajov, môžu byť mechanizmy spracovania údajov a systém auditu vytvorené tak, aby vyhovovali pravidlám o ochrane údajov. Pre kontrolóra môže byť ľahšie uplatňovať pravidlá o ochrane údajov na všetky druhy informácií v jeho súboroch, ako sa pokúšať oddeliť informácie týkajúce sa fyzických osôb od informácií týkajúcich sa právnických osôb.

IV. ČO SA STANE, AK ÚDAJE NEPATRIA DO ROZSAHU PÔSOBNOSTI DEFINÍCIE?

Ako sme videli v celom tomto dokumente, informácie sa za rôznych okolností môžu pokladať za informácie, ktoré nie sú osobnými údajmi. Tento prípad nastáva, keď sa údaje nemôžu považovať za údaje týkajúce sa jednotlivca alebo vtedy, keď jednotlivca nemožno označiť za identifikovanú alebo identifikovateľnú osobu. Ak spracovávané informácie nespadajú pod pojem „osobné údaje“, znamená to, že smernica sa neuplatňuje, podľa jej článku 3. To však neznamená, že jednotlivcov možno v konkrétnej situácii zbaviť akéhokoľvek druhu ochrany. Mali by sme zohľadniť nasledovné úvahy.

Ak sa neuplatňuje smernica, môžu sa uplatňovať vnútroštátne právne predpisy o ochrane údajov. Ako je stanovené v článku 34, smernica je určená členským štátom. Mimo jej rozsahu pôsobnosti členské štáty nepodliehajú povinnostiam, ktoré nariaďuje, najmä povinnosti uviesť do účinnosti zákony, iné právne predpisy, a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Ako však objasnil Európsky súdny dvor, nič nebráni členským štátom, aby rozšírili rozsah pôsobnosti vnútroštátnych predpisov, ktorými sa vykonávajú ustanovenia smernice, na oblasti, ktoré nie sú zahrnuté v rozsahu jej pôsobnosti za predpokladu, že to nevylučuje žiadne iné ustanovenie právnych predpisov Spoločenstva. Preto sa môže skutočne stať, že určité situácie nezahŕňajúce spracovanie osobných údajov definované v smernici podliehajú ochranným opatreniam na základe vnútroštátnych právnych predpisov. Môže sa to týkať napríklad údajov kódovaných kľúčom, bez ohľadu na to, či to sú alebo nie sú osobné údaje.

V prípadoch, v ktorých sa pravidlá o ochrane údajov neuplatňujú, môžu byť určité činnosti stále v rozpore s článkom 8 Európskeho dohovoru o ľudských právach, ktorý chráni právo na súkromný a rodinný život, z hľadiska rozsiahlej judikatúry Európskeho súdu pre ľudské práva. Iné súbory pravidiel, medzi ktoré patrí právo občianskoprávnych deliktov, trestné právo alebo antidiskriminačné právo, môžu tiež poskytnúť ochranu jednotlivcom v prípadoch, v ktorých sa neuplatňujú pravidlá o ochrane údajov a môže ísť o rôzne oprávnené záujmy.

V. ZÁVERY

Pracovná skupina poskytla v tomto stanovisku usmernenie k výkladu pojmu osobné údaje, ktorý je uvedený v smernici 95/46/ES a v súvisiacich právnych predpisoch Spoločenstva, a k tomu ako by sa mal tento pojem uplatňovať v rôznych situáciách.

V rámci všeobecnej úvahy sa uviedlo, že zámerom európskeho zákonodarcu bolo prijať široký výklad pojmu osobné údaje, ale jeho rozsah nie je neobmedzený. Malo by sa vždy pamätať na to, že cieľom pravidiel obsiahnutých v smernici je chrániť základné práva a slobody jednotlivcov, najmä ich právo na súkromie, pokiaľ ide o spracovanie osobných údajov. Tieto pravidlá boli preto vypracované tak, aby sa vzťahovali na situácie, v ktorých by práva jednotlivcov mohli byť ohrozené a mohli potrebovať ochranu. Rozsah pôsobnosti pravidiel o ochrane údajov by sa nemal nadmerne rozširovať, ale malo by sa tiež predísť neprimeranému obmedzovaniu rozsahu pojmu osobné údaje. V smernici je tento rozsah pôsobnosti definovaný vylúčením mnohých činností a smernica umožňuje flexibilitu v uplatňovaní pravidiel na činnosti, ktoré sú v rámci jej rozsahu pôsobnosti. Orgány na ochranu údajov zohrávajú hlavnú úlohu pri hľadaní primeranej rovnováhy pri tomto uplatňovaní (pozri oddiel II).

Analýza pracovnej skupiny vychádza zo štyroch hlavných „zložiek“, ktoré možno rozlíšiť v definícii „osobných údajov“: t. j. „akékoľvek informácie“, „týkajúce sa“, „identifikovaná alebo identifikovateľná“, „fyzická osoba“. Tieto prvky sú úzko prepletené a navzájom sa doplňujú, ale spolu určujú, či by sa informácia mala považovať za „osobný údaj“. Analýzu podporujú príklady z vnútroštátnej praxe európskych orgánov na ochranu údajov.

- Prvý prvok – „akékoľvek informácie“ – vyžaduje široký výklad pojmu bez ohľadu na charakter alebo obsah informácií a technickú formu, v ktorej sa prezentujú. To znamená, že objektívne aj subjektívne informácie o osobe v akejkoľvek funkcii sa môžu považovať za „osobné údaje“, a to bez ohľadu na technické médium, na ktorom sú uchované. Stanovisko sa zaoberá aj biometrickými údajmi a právnymi rozlíšeniami v prípade vzoriek ľudských tkanív, z ktorých je možné tieto informácie získať (pozri oddiel III.1).

- Druhý prvok – „týkajúce sa“ – sa doteraz často prehliadal, ale zohráva rozhodujúcu úlohu pri stanovení skutočného rozsahu pôsobnosti pojmu, najmä vo vzťahu k objektom a novým technológiám. V stanovisku sa uvádzajú tri alternatívne prvky – t. j. obsah, účel alebo výsledok – na určenie, či sa informácie „týkajú“ jednotlivca. To sa týka aj informácií, ktoré môžu mať jasný vplyv na spôsob, akým sa s jednotlivcom zaobchádza alebo akým sa jednotlivec posudzuje (pozri oddiel III.2).

- Tretí prvok – „identifikovaná alebo identifikovateľná“ (fyzická osoba) – sa zameriava na podmienky, za ktorých by sa jednotlivec mal pokladať za „identifikovateľnú“ osobu a najmä na „prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije“ kontrolór alebo ľubovoľná iná osoba na identifikáciu uvedenej osoby. Konkrétny kontext a okolnosti konkrétneho prípadu zohrávajú v tejto analýze dôležitú úlohu. Stanovisko sa zaoberá aj „pseudonymizovanými údajmi“ a využívaním „údajov kódovaných kľúčom“ v štatistickom alebo farmaceutickom výskume (pozri oddiel III.3).

- Štvrtý prvok – „fyzická osoba“ – sa zaoberá požiadavkou, aby „osobné údaje“ boli o „žijúcich jednotlivcoch“. Stanovisko sa zaoberá aj rozhraniami s údajmi o zosnulých osobách, nenarodených deťoch a právnických osobách (pozri oddiel III.4).

Stanovisko sa nakoniec zaoberá situáciou, ktorá nastáva, ak údaje nepatria do rozsahu pôsobnosti definície „osobných údajov“. V týchto prípadoch sú k dispozícii rôzne možnosti riešenia problémov vrátane vnútroštátnych právnych predpisov, ktoré môžu ísť

nad rámec pôsobnosti smernice za predpokladu, že nie sú v rozpore s ďalšími právnymi predpismi Spoločenstva (pozri oddiel IV).

Pracovná skupina vyzýva všetky zainteresované strany, aby dôkladne preštudovali usmernenie uvedené v tomto stanovisku a zohľadnili ho pri výklade a uplatňovaní ustanovení vnútroštátnych právnych predpisov v súlade so smernicou 95/46/ES.

Členovia pracovnej skupiny, väčšinou zástupcovia dozorných orgánov pre ochranu údajov na vnútroštátnej úrovni, sa zaviazali ďalej zdokonaľovať pokyny poskytnuté v tomto stanovisku v rámci svojich vlastných jurisdikcií a zabezpečiť riadne uplatňovanie ich vnútroštátnych právnych predpisov v súlade so smernicou 95/46/ES.

Pracovná skupina chce uplatňovať a zdokonaľovať usmernenie poskytnuté v tomto stanovisku vo všetkých vhodných oblastiach a starostlivo ho zohľadniť vo svojej ďalšej práci, najmä pri témach, medzi ktoré patrí správa identity v zmysle elektronickej štátnej správy a elektronického zdravotníctva, ako aj v zmysle RFID. Pokiaľ ide o RFID, pracovná skupina chce prispieť k ďalšej analýze spôsobu, akým môžu pravidlá o ochrane údajov ovplyvniť využívanie RFID, a možnej potreby doplňujúcich opatrení na zabezpečenie riadneho dodržiavania práv na ochranu údajov a záujmov v uvedenom zmysle.

Pracovná skupina by tiež privítala akékoľvek pripomienky a ohlasy od zainteresovaných strán a dozorných orgánov, pokiaľ ide o ich praktické skúsenosti s usmernením poskytnutým v tomto stanovisku, vrátane akýchkoľvek doplňujúcich príkladov k príkladom uvedeným v tomto dokumente. Skupina má v úmysle sa k tejto téme vo vhodnom čase ešte vrátiť s cieľom ďalšieho posilnenia spoločného porozumenia kľúčového pojmu osobné údaje a zabezpečenia zosúladeného uplatňovania a lepšieho vykonávania smernice 95/46/ES a súvisiacich právnych predpisov Spoločenstva.

Za pracovnú skupinu

predseda
Peter SCHAAR