



01248/07/ET
WP 136

Arvamus 4/2007 isikuandmete mõiste kohta

Vastu võetud 20. juunil

Töörühm on loodud direktiivi 95/46/EÜ artikli 29 alusel. See on Euroopa sõltumatu nõuandeorgan andmekaitse ja eraelu puutumatuse valdkonnas. Töörühma ülesanded on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaadi ülesandeid täidab Euroopa Komisjoni õigus-, vabadus- ja turvalisusküsimuste peadirektoraadi C direktoraat (tsiviilõigused, põhiõigused ja kodakondsus), B-1049 Brüssel, Belgia, kabinet nr LX-46 01/43.

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

TÖÖRÜHM ÜSIKISIKUTE KAITSEKS SEOSSES ISIKUANDMETE TÖÖTLEMISEGA,

mis on loodud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ alusel,¹

võttes arvesse kõnealuse direktiivi artiklit 29 ja artikli 30 lõike 1 punkti a ning lõiget 3 ja Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ artikli 15 lõiget 3,

võttes arvesse EÜ asutamislepingu artiklit 255 ja Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrust (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele,

võttes arvesse töörühma töökorda,

ON VASTU VÕTNUD KÄESOLEVA ARVAMUSE:

¹ EÜT L 281, 23.11.1995, lk 31, [ELT eriväljaanne 13/015, lk 355,] kättesaadav aadressil: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. SISSEJUHATUS	3
II. ÜLDISED KAALUTLUSED JA POLIITIKAKÜSIMUSED	4
III. ANDMEKAITSEDIREKTIIVIS SÄTESTATUD MÕISTE „ISIKUANDMED” ANALÜÜS	6
1. ESIMENE ELEMENT: „IGASUGUNE TEAVE”	6
2. TEINE ELEMENT: „KOHTA”	9
3. KOLMAS ELEMENT: „TUVASTATUD VÕI TUVASTATAV” [FÜÜSILINE ISIK]	12
4. NELJAS ELEMENT: „FÜÜSILINE ISIK”	21
IV. MIS JUHTUB, KUI ANDMED EI KUULU MÕISTE ALLA?	24
V. KOKKUVÕTE	24

I. SISSEJUHATUS

Töörühm on teadlik vajadusest analüüsida põhjalikult isikuandmete mõistet. ELi liikmesriikide praegusi käsitlusi iseloomustava teabe kohaselt valitsevad liikmesriikides kõnealuse mõiste oluliste tahkude käsitluses ebamäärasus ja erinevused, mis võivad mõjutada olemasolevate andmekaitsealaste õigusaktide nõuetekohast toimimist mitmesugustes olukordades. Andmekaitsereeglite kohaldamise ja tõlgendamise keskse elemendi analüüsi tulemused mõjutavad igal juhul märkimisväärselt mitut olulist küsimust ning eriti sellist valdkonda nagu identifitseerimine e-valitsuse ja e-tervishoiu ning raadiosagedustuvastuse (RFID) kontekstis.

Töörühma käesoleva arvamuse eesmärk on kujundada ühine seisukoht seoses isikuandmete mõistega ning sellega, millal ja kuidas tuleks kohaldada andmekaitsealaseid siseriiklike õigusakte. Isikuandmete mõiste ühine määratlemine tähendab määratleda, mis kuulub ja mis ei kuulu andmekaitsereeglite kohaldamisalasse. Lisaks tuleb anda suuniseid siseriiklike andmekaitsealaste õigusaktide kohaldamise kohta teatavates kogu Euroopat hõlmavates olukordades, aidates seega kaasa kõnealuste normide ühetaolisele kohaldamisele, mis on artikliga 29 loodud töörühma põhiülesanne.

Käesolevas dokumendis on analüüsi toetuseks ja selgituseks kasutatud näiteid Euroopa andmekaitseasutuste tegevusest. Enamikku näiteid on kohandatud üksnes käesolevas kontekstis kasutamise eesmärgil.

II. ÜLDISED KAALUTLUSED JA POLIITIKAKÜSIMUSED

Direktiivis on isikuandmete mõiste piiritletud laialt.

Direktiivis 95/46/EÜ (edaspidi „andmekaitse direktiiv” või „direktiiv”) on isikuandmete mõiste sätestatud järgmiselt:

„Isikuandmed – igasugune teave tuvastatud või tuvastatava füüsilise isiku (edaspidi "andmesubjekt") kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal”.

Tuleb märkida, et kõnealuses mõistes kajastub Euroopa seadusandja eesmärk piiritleda kasutatav mõiste „isikuandmed” laialt, mida järgiti kogu seadusandlikus protsessis. Komisjoni algses ettepanekus selgitati, et „vastavalt konventsioonile 108 määratletakse mõiste laialt, et see hõlmaks igasugust teavet, mida võib üksikisikuga siduda”.² Komisjoni muudetud ettepanekus märgiti, et „muudetud ettepanekus on arvesse võetud parlamendi soovi, et mõiste „isikuandmed” oleks võimalikult üldine, et see hõlmaks igasugust teavet tuvastatava isiku kohta”³ – soov, mida nõukogu ühises seisukohas⁴ ka arvesse võttis.

Direktiivi sätete eesmärk on üksikisikute kaitse.

Direktiivi 95/46/EÜ artikkel 1 ja direktiivi 2002/58/EÜ artikkel 1 nimetavad sõnaselgelt direktiivides sisalduvate normide peamise eesmärgi: kaitsta isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusse. See on väga tähtis asjaolu, mida tuleb arvesse võtta mõlemas õigusaktis sätestatud normide tõlgendamisel ja kohaldamisel. See võib mängida olulist osa otsustustes, kuidas kohaldada direktiivi sätteid puhkudel, kui üksikisiku õigused ei ole ohus, ja see võib manitseda ettevaatlikkusele kõnealuste sätete tõlgendamise suhtes viisil, mis jätab üksikisikute õigused kaitseta.

Paljud tegevused ei kuulu direktiivi reguleerimisalasse ja selle tekst on paindlik, et esinevates olukordades oleks võimalik anda sobiv õiguslik vastus.

Hoolimata sellest, et direktiivis on mõisted „isikuandmed” ja „töötlemine” piiritletud laialt, ei tähenda – eelkõige tulenevalt artiklist 3 – ainuüksi asjaolu, et teatav olukord võib olla seotud „isikuandmete töötlemisega” kõnealuse mõiste tähenduses seda, et kõnealusele olukorrale laieneksid tingimata direktiivi sätted. Ühenduse õiguse kohaldamisalast tulenevate erandite kõrval võetakse artikli 3 erandites arvesse andmete töötlemise tehnilist külge (korrastamata andmekogumite automatiseerimata töötlus) ja kasutamise eesmärki (kui seda teeb füüsiline isik isiklikel või kodustel eesmärkidel). Isegi kui tegemist on direktiivi reguleerimisalasse kuuluvate isikuandmete töötlemisega, ei pruugi kõik direktiivi sätted olla konkreetsel juhul kohaldatavad. Paljud direktiivi sätted on üpris paindlikud, et saavutada sobiv tasakaal ühelt poolt andmesubjekti õiguste kaitse ja teiselt poolt andmetöötlejate ja kolmandate isikute põhjendatud huvide ning võimaliku avaliku huvi vahel. Selliste sätete näited on artikkel 6 (säilitamisaeg sõltub andmete vajalikkusest), artikli 7 punkt f (töötlemine on

² KOM (90) 314 (lõplik), 13.9.1990, lk 19 (artikli 2 kommentaar).

³ KOM (92) 422 (lõplik), 28.10.1992, lk 10 (artikli 2 kommentaar).

⁴ Nõukogu 20. veebruari 1995. aasta ühine seisukoht (EÜ) nr 1/95, EÜT C 93, 13.4.1995, lk 20.

õigustatud tasakaalustatud huvide puhul), artikli 10 punkt c ja artikli 11 lõike 1 punkti c viimane lõik (andmesubjekti teavitamine, kui see on vajalik õiglase töötlemise tagamiseks) või artikkel 18 (teatamiskohustuse erandid).

Andmekaitsenormide kohaldamisala ei tohiks olla liiga lai.

Soovimatu tulemus oleks see, kui andmekaitseõudeid kohaldataks olukordades, millele kõnealused normid ei peaks laienema ja mille jaoks seadusandja neid ei kavandanud. Eespool nimetatud artikli 3 olulised erandid ja direktiivi 26. ja 27. põhjenduse selgitused väljendavad seadusandja tahet selle kohta, millal ja kuidas peaks kohaldama andmekaitseõudeid.

Üheks piiranguks on andmete töötlemise viis. Tuleks meenutada, et esimesed andmekaitseõudused võeti seitsmekümnendatel aastatel vastu seetõttu, et uus tehnoloogia, st elektrooniline andmetöötlus võimaldas isikuandmete lihtsamat ja laialdasemat juurdepääsu kui traditsioonilised andmete käsitlemise meetodid. Seetõttu on direktiiviga loodud andmekaitse eesmärk kaitsta selliseid töötlemise viise, mille puhul on tavaliselt suurem oht, et need võimaldavad „lihtsat juurdepääsu isikuandmetele” (27. põhjendus). Isikuandmete automatiseerimata töötlemine kuulub direktiivi reguleerimisalasse üksnes siis, kui andmed kuuluvad kataloogi või kui need kavatakse hiljem sellesse kanda (artikkel 3).

Teine üldine piirang direktiiviga tagatud andmekaitse kohaldamisele on andmete töötlemine olukorras, kus andmesubjekti tuvastamise vahendeid ei saa „tõenäoliselt kasutada” (26. põhjendus) – küsimus, mida arutatakse allpool.

Samas tuleks vältida ka isikuandmete mõiste põhjendamatult kitsendavat tõlgendust.

Juhtudel, kui direktiivi kõigi sätete mehhaaniline kohaldamine tooks esmapilgul kaasa liialt koormavaid või isegi absurdseid tagajärgi, tuleb esmalt kontrollida, 1) kas olukord on direktiivi reguleerimisalal, pidades eelkõige silmas artiklit 3, ja 2) kui see on direktiivi reguleerimisalal, kas direktiiv ise või selle alusel vastu võetud siseriiklikud õigusaktid võimaldavad konkreetses olukorras erandi tegemist või lihtsustamist, et õiguslikus mõttes adekvaatselt reageerida, tagades samas üksikisiku asjaomaste õiguste ja huvide kaitse. Isikuandmete mõiste põhjendamatult kitsendava tõlgendamise asemel tuleks pigem märkida, et kõnealuseid norme saab andmetele kohaldada väga paindlikult.

Siseriiklikel andmekaitse järelevalveasutustel on siin oluline osa, sest nende ülesanne on kontrollida andmekaitseõiguse kohaldamist, mis hõlmab õigusnormide tõlgendamist ja konkreetsete juhiste andmist vastutavatele töötlejatele ja andmesubjektidele. Nad peaksid toetama mõistet, mis on piisavalt lai, et võtta juba ette arvesse valdkonna arengut ja hõlmata „halle tsoone”, kasutades samas õiguspäraselt ära direktiivi paindlikkust. Tegelikult tingib direktiivi sõnastus selliste põhimõtete kujundamise, mis ühendavad endas isikuandmete mõiste laia tõlgenduse ja sobiva tasakaalu direktiivi sätete kohaldamisel.

III. ANDMEKAITSEDIREKTIIVIS SÄTESTATUD MÕISTE „ISIKUANDMED” ANALÜÜS

Direktiivis sätestatud mõiste toetub neljale peamisele elemendile, mida käesolevas dokumendis analüüsitakse eraldi. Need on järgmised:

- „igasugune teave”
- „tuvastatud või tuvastatav”
- „füüsiline isik”
- „kohta”

Kõnealused neli elementi on omavahel tihedalt seotud ja üksteisest sõltuvad. Käesolevas dokumendis kasutatava meetodika tõttu käsitletakse iga elementi eraldi.

1. ESIMENE ELEMENT: „IGASUGUNE TEAVE”

Direktiivis kasutatud fraas „igasugune teave” viitab selgelt seadusandja taatele luua laialt piiritletud isikuandmete mõiste. Selline sõnastus tingib mõiste laia tõlgenduse.

Teabe laadi seisukohalt hõlmab isikuandmete mõiste igasuguseid isiku kohta käivaid väiteid. Siia kuulub „objektivne teave”, näiteks mingi aine sisaldus isiku veres. See hõlmab ka „subjektiivset” teavet, arvamusi või hinnanguid. Viimast liiki väited moodustavad märkimisväärse osa isikuandmetest, mida töödeldakse näiteks panganduses laenuvõtjate hindamisel („Titius on usaldusväärne laenuvõtja”), kindlustuses („Titius elab eeldatavalt kaua”) või töösuhetes („Titius on hea töötaja ning väärib edutamist”).

Selleks et teave kujutaks endast „isikuandmeid”, ei pea see olema tingimata tõene või tõendatud. Tegelikult on andmekaitseõuded juba ette näinud võimaluse, et teave on ebaõige ja sätestavad andmesubjekti õiguse kõnealuse teabega tutvuda ning vaidlustada see asjakohaste õiguskaitsevahendite kaudu.⁵

Teabe sisu seisukohalt hõlmab isikuandmete mõiste andmeid, mis annavad mis tahes liiki teavet. See hõlmab loomulikult „delikaatseteks andmeteks” peetavat isiklikku laadi teavet direktiivi artiklis 8 selle riskidega seotud iseloomu tõttu, kuid ka muud, üldisemat teavet. Mõiste „isikuandmed” hõlmab teavet, mis puudutab üksikisiku era- ja perekonnaelu kitsamas mõttes, kuid ka teavet üksikisiku mis tahes tegevuse kohta, näiteks tema töösuhete või majandusliku või sotsiaalse käitumisega seotud teavet. Seetõttu kuulub siia teave üksikisikute kohta, sõltumata kõnealuste isikute ametikohast või kategooriast (tarbija, patsient, töötaja, klient jne).

⁵ Parandusi võib teha vastupidiste märkuste esitamisega või asjakohaste õiguskaitsevahendite kasutamisega, näiteks hagi esitamisega.

Näide nr 1. Ametialased harjumused ja tavad

Retseptiravimeid käsitlevat teavet (nt ravimi tunnuscode, ravimi nimi, ravimi tugevus, tootja, müügihind, uus või korduvretsept, kasutamise põhjused, asendamise keeldumise põhjused, ravimi välja kirjutanud isiku ees- ja perekonnanimi, telefoninumber jne), mis tuleneb ühest retseptist või mitme retsepti alusel kujundatud üldpildist, võib pidada ravimi välja kirjutanud arsti isikuandmeteks isegi juhul, kui patsient jääb anonüümseks. Seega on tuvastatud või tuvastatava arsti poolt väljakirjutatud retsepti kohta retseptiravimite tootjatele teabe andmine isikuandmete edastamine kolmandatele isikutele direktiivi tähenduses.

Sellist tõlgendust toetab ka direktiivi sõnastus. Ühelt poolt tuleb arvesse võtta, et era- ja perekonnaelu mõiste on väga lai, nagu on selgitanud Euroopa Inimõiguste Kohus.⁶ Teisalt ulatuvad isikuandmete kaitse reeglid kaugemale laiaulatusliku mõiste „õigus era- ja perekonnaelu austamisele” kaitsest. Tuleks märkida, et Euroopa Liidu põhiõiguste harta artiklis 8 on isikuandmete kaitse sätestatud eraldi õigusena, mis erineb harta artiklis 7 nimetatud õigusest eraelu puutumatusel, ja nii on ka mõne liikmesriigi siseriiklikul tasandil. See on kooskõlas artikli 1 lõikega 1, mille eesmärk on kaitsta „füüsiliste isikute põhiõigusi ja -vabadusi ja *eriti* [kuid mitte ainult] õigust eraelu puutumatusel”. Seepärast nimetab direktiiv eraldi isikuandmete töötlemist väljaspool kodu ja perekonda, näiteks seoses tööõigusega (artikli 8 lõike 2 punkt b), kriminaal- ja halduskaristuste või tsiviilasjades tehtud kohtuotsustega (artikli 8 lõige 5) või otseturustamisega (artikli 14 punkt b). Euroopa Kohus on toetanud sellist laiapõhjalist käsitlust.⁷

Peatudes teabe vormingul või -kandjal, tuleb märkida, et isikuandmete mõiste laieneb mis tahes vormis teabele: see võib esineda sõnadena, numbritena, graafiliselt, fotona või helina. Teave võib esineda näiteks paber kandjal, samuti arvuti mälus kahendkoodis või näiteks videol. See on automatiseeritud andmetöötluse direktiivi reguleerimisalasse lisamise loogiline tagajärg. Eeskätt on sellise käsitluse järgi isikuandmed ka heli- ja pildiaandmed, sest need võivad anda isiku kohta teavet. Seda, et direktiivi artiklis 33 on eraldi nimetatud heli- ja pildiaandmed, tuleb mõista kinnitusena ja selgitusena selle kohta, et sellised andmed kuuluvad tööpoolest direktiivi reguleerimisalasse (kui kõik muud tingimused on täidetud) ja et direktiivi kohaldatakse ka nende suhtes. Tegelikult on see kõnealuse artikli, mille eesmärk on hinnata, kas direktiivi sätted annavad sobiva õigusliku vastuse kõnealustes valdkondades, loogiline eeldus. Seda selgitab täiendavalt 14. põhjendus, märkides, et „võttes arvesse infoühiskonnas praegu toimuvat füüsiliste isikutega seotud heli- ja pildiaandmete kogumise, edastamise, töötlemise, salvestamise, talletamise ja vahendamise tehnoloogia arengut ja sellise arengu olulisust, peaks

⁶ Euroopa Inimõiguste Kohtu 16. veebruari 2000. aasta otsus kohtuasjas Amann vs. Šveits, punkt 65 : „[...] mõistet „eraelu” ei tohi tõlgendada kitsendavalt. Eraelu austamine hõlmab teiste inimestega suhete loomise ja arendamise õigust; lisaks ei õigusta ükski põhimõte ametialase või ärilise iseloomuga tegevuste väljajätmist mõistest „eraelu” (vt 16. detsembri 1992. aasta otsus kohtuasjas Niemietz vs. Saksamaa, seeria A nr 251-B, lk 33-34, punkt 29, ja eespool viidatud Halfordi kohtuotsus, lk 1015-16, punkt 42). Kõnealune lai tõlgendus on kooskõlas Euroopa Nõukogu 28. jaanuari 1981. aasta konventsiooni tõlgendusega [...]”

⁷ Euroopa Kohtu 6. novembri 2003. aasta otsus kohtuasjas C-101/2001: Lindqvist (EKL 2003, lk I-12971, lk 87), punkt 24: „Direktiivi 95/46 artikli 3 lõikes 1 kasutatud mõiste „isikuandmed” hõlmab artikli 2 punkti a kohaselt igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta. Mõiste hõlmab kahtlemata isiku nime seostatuna tema telefoninumbri või teabega tema töötingimuste või hobide kohta”.

käesolev direktiiv olema kohaldatav ka selliste andmete töötlemise suhtes”. Teisalt ei pea teave esinema korrastatud andmebaasis või toimikus, et seda käsitataks isikuandmetena. Ka elektroonilises dokumendis vaba tekstina esitatud teavet võib käsitada isikuandmetena, kui on täidetud isikuandmete mõiste muud kriteeriumid. Näiteks sisaldab „isikuandmeid” elektronpost.

Näide nr 2. Telefonipangandus

Telefonipanganduses, kus pangale korraldusi andva kliendi hääl salvestatakse, tuleks kõnealuseid salvestatud korraldusi käsitada isikuandmetena.

Näide nr 3. Videovalve

Videovalve süsteemi salvestatud isikute kujutised võivad olla isikuandmed, kui kõnealused isikud on äratuntavad.

Näide nr 4. Lapse joonistus

Hooldusõigust käsitlevas kohtumenetluses tehti tüdrukuga neuro-psühhiaatriline test, mille tulemusena esitatakse tüdruku joonistus, millel on kujutatud tema perekond. Joonistus annab teavet tüdruku meeleolu kohta ja selle kohta, millised on tema tunded eri pereliikmete vastu. Sellisena tuleks joonistust käsitada „isikuandmetena”. Joonistus annab teavet lapse kohta (tema vaimse tervise kohta) ja ka näiteks tema isa või ema käitumise kohta. Järelikult võivad vanemad nimetatud kohtuasjas kasutada oma õigust tutvuda kõnealuse teabega.

Siinkohal tuleks eraldi viidata biomeetrilistele andmetele. Neid võib määratleda bioloogiliste, füsioloogiliste või iseloomustavate tunnustena või korduvate tegevustena, kusjuures need tunnused ja/või tegevused on nii kõnealusele isikule ainuomased kui ka mõõdetavad, isegi kui praktikas kaasneb nende tehnilisel mõõtmisel kasutatavate meetoditega mõningane tõenäosus. Selliste biomeetriliste andmete tüüpiliseks näiteks on sõrmejäljed, silma võrkkest, näokujutis, hääl, aga ka käegeommeetria, veresoonte muster või isegi sügavalt juurdunud oskus või käitumuslik tunnus (näiteks omakäeline allkiri, klahvivajutused, iseloomulik kõndimisviis või kõnemaneeer jne)

Biomeetrilistele andmetele on iseloomulik, et neid võib pidada nii konkreetset üksikisikut käsitlevate andmete *sisuks* (need on Titiusse sõrmejäljed) kui ka elemendiks, mille abil saab tuvastada *seose* mingi teabe ning isiku vahel (seda eset on puudutanud keegi, kellel on sellised sõrmejäljed ja need sõrmejäljed langevad kokku Titiusse omadega; seega puudutas eset Titius). Sellisena toimivad need „tunnusena”. Tõepoolest, biomeetrilisi andmeid võib nende ainulaadse seose tõttu konkreetse isikuga kasutada kõnealuse isiku tuvastamiseks. Duaalsus iseloomustab ka DNA andmeid, mis annavad teavet inimkeha kohta ja võimaldavad samas isiku ühemõttelist ning ainukordset tuvastamist.

Inimkudede proovid (näiteks vereproovid) on mõnikord biomeetriliste andmete allikad, kuid need ei ole iseenesest biomeetrilised andmed (näiteks on biomeetrilised andmed sõrmejäljed, kuid mitte sõrmed). Seetõttu on teabe kogumine proovidest isikuandmete

kogumine, millele kohaldatakse direktiivi nõudeid. Koeproovide säilitamisele ja kasutamisele võidakse kohaldada teistsuguseid nõudeid.⁸

2. TEINE ELEMENT: „KOHTA”

Mõiste see element on vajalik, et täpsustada, millised suhted/seosed on olulised ja kuidas neid eristada.

Üldiselt käib teave üksikisiku „kohta”, kui see on seotud kõnealuse isikuga.

Paljudel juhtudel on seos kergesti tuvastatav. Näiteks personaliosakonnas isiku toimikusse kantud andmed on ühemõtteliselt seotud kõnealuse isiku kui töötaja seisundiga. Sama kehtib ka patsiendi tervisekontrolli kaardile kantud meditsiiniliste analüüside tulemuste kohta või videointervjuu käigus salvestatud isiku kujutise kohta.

Mainida võiks mitmeid teisigi olukordi, kuigi alati ei ole see, kas teave käib isiku „kohta”, nii iseenesest mõistetav kui eespool nimetatud juhtudel.

Mõnikord edastavad andmed teavet, mis puudutab esmajoones esemeid, mitte isikuid. Tavaliselt kuuluvad kõnealused esemed kellelegi või mõjutab neid konkreetselt mõni isik või mõjutavad need mõnda isikut või asuvad need isiku või teiste esemete füüsilises või geograafilises läheduses. Sellisel juhul võib teavet pidada vaid kaudselt seotuks kõnealuste isikute või esemetega.

Näide nr 5. Maja väärtus

Konkreetses maja väärtus on teave eseme kohta. On selge, et andmekaitse nõudeid ei kohaldata, kui kõnealust teavet kasutatakse üksnes teatava piirkonna kinnisvarahindade näitlikustamiseks. Teatud kindlatel asjaoludel tuleks aga sellist teavet samuti käsitada isikuandmetena. Maja kuulub selle omaniku vara hulka, mistõttu seda saab kasutada näiteks kõnealuse isiku maksukohustuse ulatuse määramisel. Sellisel juhul tuleks kõnealust teavet kahtlemata käsitada isikuandmetena.

Samasugust analüüsi saab kasutada siis, kui andmed kajastavad eelkõige protsesse või sündmusi, näiteks teave masina töö kohta, kui on vajalik inimese sekkumine. Teatud asjaoludel on võimalik, et kõnealune teave käib ka üksikisiku „kohta”.

Näide nr 6. Auto hooldusraamat

Auto hooldusraamat, millesse teeb kandeid mehhaanik või remonditöökoda, hõlmab teavet auto, läbisõidu, hoolduse kuupäevade, tehniliste probleemide ja auto seisukorra kohta. Kõnealune teave on dokumentides seotud auto registreerimismärgi ja mootori numbriga, mis omakorda on seostatavad omanikuga. Kui töökoda loob arve esitamiseks sõiduki ja selle omaniku vahel seose, käib teave omaniku või juhi „kohta”. Kui andmed seostatakse autot remontinud mehhaanikuga viimase töö üle arvestuse pidamiseks, käivad andmed ka mehhaaniku „kohta”.

Töörühm on juba pööranud tähelepanu küsimusele, millal võib teavet pidada isiku „kohta” käivaks. Aruteludes, mis käsitlesid RFID-sildiga seotud andmekaitseprobleeme, märkis töörühm, et „andmed käivad üksikisiku kohta, kui need

⁸ Vt Euroopa Nõukogu Ministrite Komitee 15. märtsi 2006. aasta soovitus liikmesriikidele nr Rec (2006) 4, mis käsitleb inimpäritolu bioloogilise materjali uurimist.

viitavad tema isikule, omadustele või käitumisele või kui sellist teavet kasutatakse, et määrata või mõjutada seda, kuidas kõnealust isikut koheldakse või hinnatakse”⁹.

Tuginedes eespool kirjeldatud juhtumitele ning arendades teemat edasi, võib märkida, et selleks, et andmeid saaks pidada üksikisiku „kohta” käivaks, peab esinema element „**sisu**” VÕI element „**eesmärk**” VÕI element „**tulemus**”.

„**Sisu**” on olemas siis, kui teavet antakse konkreetse isiku kohta (vastavalt ühiskonnas levinud kõige ilmsemale ja üldisemale arusaamale sõnast „kohta”), sõltumata vastutava töötaja või kolmanda isiku eesmärgist või sellest, kuidas kõnealune teave andmesubjekti mõjutab. Teave käib isiku „kohta”, kui see on kõnealuse isikuga „seotud” ja seda hinnates tuleb arvesse võtta kõiki juhtumi asjaolusid. Näiteks on selge, et meditsiiniliste analüüside tulemused on seotud patsiendiga ja ettevõtte infosüsteemis kliendi nime all sisalduv teave on seotud viimasega. Samuti on isikut tõendavasse dokumenti kantud RFID-sildis või ribakoodis, näiteks tulevikus väljastatavates raadiosagedustuvastuse kiibiga varustatud passides sisalduv teave seotud kõnealuse isikuga.

Teave võib olla teatud isikuga seotud ka „**eesmärgi**” tõttu. „Eesmärk” on olemas, kui konkreetse juhtumi asjaolusid arvesse võttes võidakse andmeid kasutada üksikisiku hindamise, teatud viisil kohtlemise või tema seisundi või käitumise mõjutamise eesmärgil.

⁹ Töörühma dokument nr WP 105: „RFID-tehnoloogiaga seotud andmekaitseküsimused”, vastu võetud 19. jaanuaril 2005. aastal, lk 8.

Näide nr 7. Telefonikõnede eristus

Ettevõttesisene telefonikõnede eristus annab teavet kindla liiniga ühendatud telefonilt tehtud kõnede kohta. Kõnealust teavet võib seostada eri subjektidega. Ühelt poolt on liin eraldatud ettevõttele ja ettevõtte on lepinguga kohustatud kõnede eest maksma. Tööajal kasutab telefoni konkreetne töötaja ja eeldatavasti on need tema kõned. Samuti võib kõneeristus anda teavet inimese kohta, kellele helistati. Töötaja äraolekul võib telefoni kasutada ka ükskõik milline muu isik, kellel on lubatud ruumides viibida (näiteks koristaja). Teavet kõnealuse telefoniaparaadi kasutamise kohta võib erinevatel eesmärkidel seostada ettevõtte, töötaja või koristajaga (näiteks selleks, et kontrollida, mis ajal koristajad lahkusid töökohalt, sest ta peab enne ruumide lukustamist telefoni teel kinnitama töökohalt lahkumise kellaaja). Tuleks märkida, et isikuandmete mõiste laieneb siin nii väljaminevatele kui ka sissetulevatele kõnedele, sest need kõik sisaldavad teavet inimeste eraelu, sotsiaalsete suhete ja suhtlemise kohta.

Kolmandaks toimub konkreetse isikuga „seostamine” „**tulemus**” olemasolul. Hoolimata „sisu” või „eesmärgi” puudumisest, võib andmeid pidada üksikisikuga seotuks, sest nende kasutamine võib konkreetse juhtumi kõiki asjaolusid arvesse võttes mõjutada isiku õigusi ja huve. Tuleks märkida, et võimalik mõju ei pea olema suur. Piisab, kui selliste andmete töötlemise tulemusel võidakse isikut kohelda teistest erinevalt.

Näide nr 8. Takso asukoha jälgimine teenuse optimeerimiseks mõjutab juhte

Taksoettevõtte võtab kasutusele satelliidi abil asukoha määramise süsteemi, mis võimaldab reaajas määrata vabade taksode asukoha. Andmete töötlemise eesmärk on pakkuda paremat teenust ja säästa kütust, määrates igale takso kutsunud kliendile tema asukohale lähima sõiduki. Rangelt võttes on süsteemi toimimiseks vajalikud andmed, mis käivad sõidukite, mitte juhtide kohta. Andmete töötlemise eesmärk ei ole mitte taksojuhtide tegevuse hindamine, näiteks nende marsruudi optimeerimisega. Samas võimaldab süsteem jälgida taksojuhtide tegevust ja kontrollida, kas nad peavad kinni kiirusepiirangutest, valivad sobiva marsruudi, on rooli taga või puhkavad väljas jne. Seega võivad andmed kõnealuseid isikuid oluliselt mõjutada ja selliseid andmeid võib pidada füüsilise isiku kohta käivaks. Andmete töötlemine peab toimuma vastavalt andmekaitseõuetele.

Nimetatud kolm elementi (sisu, eesmärk, tulemus) on alternatiivsed, mitte kumuleeruvad tingimused. Eriti sisu olemasolu puhul ei ole teiste elementide olemasolu vajalik selleks, et seostada teavet üksikisikuga. Lisaks võivad samad andmed olla samal ajal seotud eri isikutega, sõltuvalt sellest, milline element igäihe puhul esineb. Sama teave võib „sisu” tõttu olla seotud Titiusse nimelise isikuga (andmed käivad ühemõtteliselt Titiusse kohta) JA „eesmärgi” tõttu Gaiusega (teavet kasutatakse selleks, et kohelda Gaiust erinevalt) JA „tulemus” tõttu Semproniussega (teave võib mõjutada Semproniusse õigusi ja huve). See tähendab ka, et andmed ei pea „keskenduma” konkreetsele isikule, et neid pidada temaga seotuks. Eelnevast analüüsist tulenevalt tuleb küsimusele, kas andmed käivad isiku kohta, vastata iga konkreetset andmeühikut eraldi hinnates. Sama moodi tuleks oluliste sätete (näiteks andmetega tutvumise õiguse ulatus) kohaldamisel meeles pidada asjaolu, et teave võib olla seotud eri isikutega.

Näide nr 9. Koosoleku protokollis sisalduvad andmed

Eespool nimetatud vajadus analüüsida kõiki andmeid eraldi puudutab teavet, mis sisaldub koosoleku protokollis, kuhu tavaliselt märgitakse osalejad Titius, Gaius ja Sempronius; Titiuse ja Gaiuse märkused ning aruanne käsitletud teemade kohta, mille kokkuvõtte teeb protokollija Sempronius. Titiusega seotud isikuandmeteks saab pidada ainult teavet, et ta osales koosolekul, mis toimus teatud ajal ja teatud kohas, ning esitas teatud märkused. Gaiuse kohalolek, tema märkused ja Semproniuse koostatud kokkuvõtte EI OLE Titiusega seotud isikuandmed. See on nii isegi juhul, kui kõnealune teave sisaldub samas dokumendis ja isegi kui see oli Titius, kes andis tõuke küsimuse koosolekul arutamiseks. Seetõttu ei hõlma Titiuse õigus tutvuda isikuandmetega kõnealust teavet. Kas ja mil määral saab kõnealust teavet pidada Gaiuse ja Semproniuse isikuandmeteks, tuleb kindlaks teha eraldi, kasutades eespool kirjeldatud analüüsi.

3. KOLMAS ELEMENT: „TUVASTATUD VÕI TUVASTATAV” [FÜÜSILINE ISIK]

Direktiiv nõuab, et teave peab olema seotud „tuvastatud või tuvastatava” füüsilise isikuga. Sellest tulenevad järgmised kaalutlused.

Üldjuhul võib füüsilist isikut pidada „tuvastatuks”, kui teda „eristatakse” teistest isikute rühma liikmetest. Järelikult on veel tuvastamata füüsiline isik „tuvastatav”, kui seda on võimalik teha (seda näitab järelliide „-tav”). Seega on kõnealune teine võimalus tegelikult otsustav tingimus, mis määrab, kas teavet iseloomustab kolmas element.

Tuvastamine toimub tavaliselt konkreetse teabe alusel, mida võib nimetada „tunnusteks” ja mis on konkreetse isikuga eriti tihedalt seotud. Näitena võib tuua kõnealuse isiku välised tunnused, näiteks pikkus, juuste värv, riietus jne või omadused, mida ei saa otsekohe tajuda, näiteks amet, tegevus, nimi jne. Direktiivis nimetatakse kõnealuseid „tunnuseid” artiklis 2 sätestatud „isikuandmete” mõistes, kus on öeldud, et füüsilist isikut „saab tuvastada otseselt või kaudselt, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal”.

„Otseselt” või „kaudselt” tuvastatav

Täiendav selgitus on esitatud komisjoni muudetud ettepaneku artiklite märkustes, milles on öeldud, et „isiku võib tuvastada otseselt nime alusel või kaudselt telefoninumbri, auto registreerimisnumbri, isikukoodi, passi numbri või oluliste kriteeriumite kombinatsiooni alusel, mis võimaldavad teda ära tunda, piirates rühma, kuhu ta kuulub (vanus, amet, elukoht jne)”. Kõnealusest sedastusest ilmneb, et see, mil määral on mingid tunnused tuvastamiseks piisavad, sõltub mõnevõrra konkreetsest olukorrast. Väga levinud perekonnanimest ei piisa isiku tuvastamiseks, st riigi elanikkonna seast kellegi esile tõstmiseks, samas kui selle alusel on võimalik tuvastada klassi õpilane. Inimese võib teiste valgusfoori taga seisvate inimeste seas tuvastada isegi kõrvalise teabe põhjal (näit „mustas ülikonnas mees”). Seega sõltub see, kas isik, kelle kohta teave käib, tuvastatakse või mitte, juhtumi asjaoludest.

„Otseselt” tuvastatud või tuvastatava isiku kohta peab märkima, et isiku **nimi on** tõepoolest kõige tavalisem tunnus ja tegelikult tähendab mõiste „tuvastatud isik” kõige sagedamini, et teada on isiku nimi.

Isikusamasuses veendumiseks tuleb isiku nimi mõnikord siduda muude andmetega (sünnikuupäev, vanemate nimed, aadress või näofoto), et vältida tema segiajamist võimalike nimekaimudega. Näiteks teavet, et Titius on rahasumma võlgu, võib pidada tuvastatud isikuga seotuks, sest sellel on seos kõnealuse isiku nimega. Nimi on teave, mis näitab, et isik kasutab kõnealust tähtede ja häälikute kombinatsiooni iseenda eristamiseks ja selleks, et teised isikud, kellega ta suhtleb, teda eristaksid. Samuti võib nime alusel leida teavet selle kohta, kus kõnealune isik elab või kust teda leida võib, kes kuuluvad tema perekonda (perekonnanime kaudu) ja kõnealuse nimega seotud mitmesuguste õigus- ja ühiskondlike suhete kohta (haridust tõendavad dokumendid, tervisekontrolli kaart, pangakontod). Kui nimele on lisatud isiku pilt, võib saada teavet isegi tema välimuse kohta. Kõik nimega seostatud lisaandmed võimaldavad detailideni tutvuda luust ja lihast isikuga ja seetõttu seostatakse algne teave tunnuste alusel füüsilise isikuga, keda saab eristada teistest isikutest.

„Kaudselt” tuvastatud või tuvastatava isiku kohta peab märkima, et see kategooria on tavaliselt seotud nähtusega, mida nimetatakse „unikaalseks kombinatsiooniks”, olgu see siis väike või suur. Juhtudel, kus esmapilgul tundub, et olemasolevad tunnused ei võimalda konkreetset isikut välja selgitada, võib isik olla siiski „tuvastatav”, sest kõnealune teave koos muude andmetega (sõltumata sellest, kas vastutav töötleja viimaseid säilitab või mitte) võimaldab isikut teistest eristada. Just sellele viitab direktiiv fraasiga „üks või mitu tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omast joont”. Mõned tunnused on nii ainulaadsed, et isik on raskusteta tuvastatav („Hispaania praegune peaminister”), kuid mõnikord võib üksikasjade kombinatsioon kategooria tasandil (vanus, piirkondlik päritolu jne) anda üpris hea tulemuse, eriti kui on olemas juurdepääs mingisuguselegi lisateabele. Statistikud on kõnealust nähtust palju uurinud, jälgides alati hoolikalt, et ei rikutaks konfidentsiaalsust.

Näide nr 10. Ajakirjanduses avaldatud osaline teave

Avaldatakse teave varem suurt avalikkuse tähelepanu pälvinud kriminaalasja kohta. Artiklis ei nimetata ühtegi tavapärasest tunnust, rääkimata asjaomase isiku nimest või sünnikuupäevast.

Tundub, et ei ole kuigi raske koguda lisateavet, mis võimaldab teha kindlaks, kes on juhtumiga seotud isikud; näiteks võib lugeda toonaseid ajalehti. Tõepoolest, pole sugugi võimatu, et keegi kasutab seda võimalust (uurib vanu ajalehti), mistõttu ta tõenäoliselt leiab näites nimetatud isikute nimed ja muud tunnused. Seega tundub olevat põhjendatud, et näites nimetatud teavet saab pidada „teabeks tuvastatava isiku kohta” ja seega „isikuandmeteks”.

Siinkohal tuleks märkida, et kuigi tegelikkuses toimub tuvastamine kõige sagedamini nime abil, ei tarvitse nimi ise alati olla isiku tuvastamiseks vajalik. See võib olla nii, kui kellegi isiku väljaselgitamiseks kasutatakse teisi „tunnuseid”. Tõepoolest, arvutifailides, kus isikuandmed registreeritakse, omistatakse registreeritud isikule tavaliselt ainukordne tunnus, et vältida kahe registreeritud isiku segiajamist. Samuti on Internetiliikluse jälgimise vahenditega kerge tuvastada arvuti ja seega ka selle kasutaja käitumist. Nii pannakse isiksusest kokku pilt, mis võimaldab talle omistada teatavad otsused. Isegi isiku nime või aadressi küsimata on võimalik liigitada ta sotsiaalmajanduslike, psühholoogiliste, filosoofiliste ja muude näitajate põhjal ning omistada talle teatud otsused, sest isiku kontaktpunkt (arvuti) ei vaja enam tingimata tema isikusamasuse avaldamist kitsamas mõttes. Teisisõnu ei sõltu isiku tuvastamine enam tingimata võimalusest saada teada tema nimi. Seda asjaolu kajastab isikuandmete mõiste.¹⁰

Euroopa Kohus on selles suhtes leidnud, et „Internetileheküljel mitmesugustele isikutele viitamine ja nende tuvastamine nime abil või muul viisil, näiteks nende telefoninumbri või nende töötingimusi ja hobisid käsitleva teabe avaldamisega, kujutab endast isikuandmete töötlemist [...] direktiivi 95/46/EÜ tähenduses”.¹¹

Näide nr 11. Varjupaigataotlejad

Oma tegelikku nime varjavatele varjupaigataotlejatele antakse vastuvõtukeskuses haldusotstarbel kood. See kood on tunnus, millega seostatakse varjupaigataotleja asutuses viibimisega seotud erinevad andmed, ning foto või muude biomeetriliste andmete abil on kõnealune kood tihedalt ja vahetult füüsilise isikuga seotud, võimaldades teda eristada teistest varjupaigataotlejatest ja seostada temaga erinevaid andmeid, mis viitavad „tuvastatud” füüsilisele isikule.

Artikli 8 lõikes 7 on samuti sätestatud, et „liikmesriigid määravad kindlaks tingimused, mille kohaselt võib töödelda siseriiklikku isikukoodi või muud üldkasutatavat tunnus”. Tasub märkida, et kõnealune säte, mis ei täpsusta, millised tingimused liikmesriigid

¹⁰ Aruanne Euroopa Nõukogu üksikisikute kaitset isikuandmete automaattöötlemisel käsitleva konventsiooni nõuandekomiteele andmekaitsepõhimõtete kohaldamise kohta ülemaailmsetes telekommunikatsioonivõrkudes, autor: Yves POULLET ja tema meeskond, punkt 2.3.1, T-PD (2004) 04 lõplik

¹¹ Euroopa Kohtu 6. novembri 2003. aasta otsus kohtuasjas C-101/2001: Lindqvist (EKL 2003, lk I-12971, lk 87, punkt 27).

peaksid kindlaks määrama, on paigutatud delikaatseid isikuandmeid käsitlevasse artiklisse. 33. põhjenduses nimetatakse selliseid andmeid andmeteks, „mis oma olemuse tõttu võivad rikkuda põhivabadusi või eraelu puutumatust”. On põhjust arvata, et seadusandjal olid sarnased kahtlused seoses siseriiklike isikukoodidega, kuna lihtsuse tõttu on väga tõenäoline, et isikukood võidakse üheselt siduda mitmesuguse teabega asjaomase isiku kohta.

Tuvastamisvahendid

Erilist tähelepanu pööratakse mõistele „tuvastatav” direktiivi 26. põhjenduses, milles on öeldud, et „isiku tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida volitatud töötleja [õige termin – „vastutav töötleja“] või keegi muu võib andmesubjekti tuvastamiseks tõenäoliselt kasutada.” See tähendab, et üksnes üksikisiku eristamise hüpoteetilisest võimalusest ei piisa, et lugeda kõnealune isik „tuvastatavaks”. Kui „kõiki vahendeid, mida vastutav töötleja või keegi muu võib [...] tõenäoliselt kasutada,” arvesse võttes selline võimalus puudub või see on väike, ei peeta isikut „tuvastatavaks” ja teavet „isikuandmeteks”. Kriteeriumis „kõik vahendid, mida vastutav töötleja või keegi muu võib [...] tõenäoliselt kasutada” tuleks eriti arvesse võtta kõiki asjaomaseid tegureid. Tuvastamise maksumus on üks tegur, kuid mitte ainus. Arvesse tuleb võtta ka kavandatud eesmärki, töötlemise liigendatust, vastutava töötleja ootusi, üksikisikute huve ja organisatsioonilisi häireid (nt konfidentsiaalsuskohustuse rikkumine) ning tehnilisi rikkeid. Teisalt on test dünaamiline ja peaks arvesse võtma töötlemise ajal kasutatavat uusimat tehnoloogiat ning seda, kuidas see võib areneda aja jooksul, mil andmeid töödeldakse. Tuvastamine ei pruugi olla võimalik praegu, võttes arvesse vahendeid, mida praegu tõenäoliselt võidakse kasutada. Kui andmeid säilitatakse üks kuu, eeldatakse, et tuvastamine ei ole teabe „eluea” jooksul võimalik ja seda ei peaks käsitlema isikuandmetena. Kui aga andmeid kavatakse säilitada 10 aastat, peaks vastutav töötleja arvestama, et tuvastamine võib toimuda andmete eluea üheksandal aastal, mis võib need siis muuta isikuandmeteks. Süsteemi peaks olema võimalik vastavalt toimunud arengule kohandada ja sellesse peaks saama õigeaegselt teha asjakohaseid tehnilisi ja organisatsioonilisi muudatusi.

Näide nr 12. Röntgenipiltide avaldamine koos patsiendi eesnimega

Naise röntgenipilt avaldati teadusajakirjas koos tema väga ebatavalise eesnimega. Isiku eesnimi, millele lisandus tema sugulaste ja tuttavate teadmine, et ta on põdenud teatud haigust, muutis isiku paljude inimeste jaoks tuvastatavaks ning röntgenipilti oleks tulnud käsitada isikuandmetena.

Näide nr 13. Ravimiüuringu andmed

Haiglad või perearstid annavad oma patsientide terviseandmed äriühingule meditsiiniüuringute eesmärgil. Patsientide nimesid ei kasutata, igale kliinilisele juhtumile antakse ainult seerianumber, et tagada järjepidevus ja vältida eri patsientide andmete segiajamist. Patsientide nimed on teada üksnes nende arstile, kes on kohustatud hoidma arstisaladust. Andmed ei sisalda lisateavet, mille kombineerimisel oleks võimalik patsiente tuvastada. Lisaks rakendatakse kõikvõimalikke meetmeid, olgu need siis õiguslikud, tehnilised või organisatsioonilised, et vältida andmesubjektide tuvastamist või tuvastatavaks muutumist. Sellistel asjaoludel võib andmekaitseasutus leida, et ravimitootjal puuduvad andmete töötlemisel vahendid, mida oleks võimalik kasutada andmesubjektide tuvastamiseks.

Nagu eespool nimetatud, on üheks oluliseks teguriks, mille alusel hinnata „kõiki vahendeid, mida võidakse tõenäoliselt kasutada” isiku tuvastamiseks, tegelikult eesmärk, mida vastutav töötleja soovib andmete töötlemisega saavutada. Liikmesriikide andmekaitseasutused on tegelenud juhtumitega, kus ühelt poolt töötleja väidab, et töödeldakse üksnes hajutatud andmeid viiteta nimele või muudele otsestele tunnustele, ning kinnitab, et andmeid ei tuleks käsitada isikuandmetena ning nende suhtes ei peaks kohaldama andmekaitseõudeid. Teisalt on teabe töötlemisel mõte üksnes siis, kui see võimaldab tuvastada konkreetseid isikuid ja neid teatud viisil kohelda. Sellistel juhtudel, kus töötlemise eesmärk nõuab, et isikud tuleb tuvastada, võib eeldada, et vastutaval töötlejal või muul asjaomasel isikul on vahendid „mida võidakse tõenäoliselt kasutada” andmesubjekti tuvastamiseks. Tegelikult oleks väide, et üksikisikud ei ole tuvastatavad, kui andmete töötlemise eesmärk on just nende tuvastamine, selge mõistete vastuollu seadmine. Seetõttu tuleks teavet käsitleda teabena tuvastatava füüsilise isiku kohta ja andmete töötlemisele tuleks kohaldada andmekaitseõudeid.

Näide nr 14. Videovalve

Videovalve puhul on see eriti oluline, sest vastutavad töötlejad väidavad sageli, et tuvastamine toimub ainult väikese osa kogutud materjali puhul ja seetõttu enne seda, kui nendel vähestel juhtudel tuvastamine tegelikult toimub, isikuandmeid ei töödelda. Kuna videovalve eesmärk on siiski videol kujutatud isikute tuvastamine alati, kui vastutav töötleja peab seda vajalikuks, tuleb kogu rakendust käsitada tuvastatavate isikute andmete töötlemisena, isegi kui mõned videole jäänud isikud ei ole tegelikult tuvastatavad.

Näide nr 15. Dünaamilised IP-aadressid

Töörühm käsitab IP-aadresse andmetena tuvastatava isiku kohta. Ta on öelnud, et „Internetiaadresside pakkujad ja kohtvõrkude haldajad saavad mõistlikke vahendeid kasutades tuvastada Internetikasutajad, kes on saanud neilt IP-aadressi, sest nad registreerivad süstemaatiliselt kuupäeva, kellaaja, kestuse ja Internetikasutajale antud dünaamilise IP-aadressi. Sama kehtib ka Internetiteenuste pakkujate kohta, kes peavad arvestust HTTP serveri kasutamise üle. Sellistel juhtudel võib kahtlemata rääkida isikuandmetest direktiivi artikli 2 punkti a tähenduses ...”¹²

Eriti siis, kui IP-aadresse töödeldakse arvutikasutajate tuvastamise eesmärgil (näiteks kui seda teevad autoriõiguste omanikud, et leida arvutikasutajad, kes rikuvad intellektuaalomandi õigusi), eeldab vastutav töötleja, et näiteks kohtul, kus asja menetletakse, on olemas „vahendid, mida võidakse tõenäoliselt kasutada” isikute tuvastamiseks (muidu ei oleks teabe kogumisel mingit mõtet), ja seetõttu tuleks teavet käsitada isikuandmetena.

Erijuhtumina ei võimalda teatavad IP-aadressid mitmesugustel tehnilistel ja organisatsioonilistel põhjustel tõepoolest kasutajat tuvastada. Üheks näiteks on IP-aadressid, mis on antud arvutitele Internetikohvikus, kus ei nõuta kliendi isiku tuvastamist. Võib väita, et andmed, mis on kogutud x arvuti kasutamise kohta teatud aja jooksul, ei võimalda kasutajat mõistlike vahenditega tuvastada ja seega ei ole tegemist isikuandmetega. Tuleks siiski märkida, et Internetiteenuse pakkujad ei tea tõenäoliselt, kas asjaomane IP-aadress võimaldab tuvastamist või mitte, ja nad

¹² WP 37: Privaatsus Internetis - võrguandmete kaitse ühetaoline käsitlemine ELis - vastu võetud 21. novembril 2000. aastal.

töötlevad kõnealuse IP-ga seotud andmeid sama moodi nagu neid, mis on seotud IP-aadressi kasutajatega, kes on nõuetekohaselt registreeritud ja tuvastatavad. Seega tuleb kõiki IP-aadressidega seotud andmeid käsitleda igaks juhuks isikuandmetena, v.a juhul, kui Internetiteenuse pakkuja suudab absoluutse kindlusega kindlaks teha, et andmed on seotud kasutajaga, keda ei ole võimalik tuvastada.

Näide nr 16. Grafitiga põhjustatud kahju

Reisijateveoks kasutatavaid veoettevõtte sõidukeid rikutakse sageli grafitiga. Kahju hindamiseks ja kahju põhjustajate vastu õiguskaitsevahendite kasutamise ettevalmistamiseks loob ettevõtte registri, mis sisaldab teavet kahju tekkimise asjaolude kohta, kahjustatud esemete pilte ja grafiti autorite „tunnusmärke” või „allkirju”. Andmete registrisse kandmise ajal ei ole teada, kes on kahju põhjustajad või kellele „allkiri” kuulub. Võib juhtuda, et seda ei saadagi kunagi teada. Andmete töötlemise eesmärk on siiski just isikute tuvastamine, kellega teave on seotud kui kahju põhjustajatega, et nende vastu oleks võimalik kasutada õiguskaitsevahendeid. Sellisel töötlemisel on mõte, kui vastutav töötleja eeldab, et „tõenäoliselt” suudetakse isik ühel päeval tuvastada. Piltides sisalduvat teavet tuleks käsitada teabena „tuvastatavate” isikute kohta, registris sisalduvat teavet „isikuandmetena” ja andmete töötlemisele tuleks kohaldada andmekaitseõudeid, mille kohaselt on selline töötlemine teatud asjaoludel seaduslik ning mille puhul tuleb rakendada teatavaid kaitsemeetmeid.

Kui töötlemise eesmärk ei ole andmesubjekti tuvastamine, etendavad väga olulist osa tuvastamist takistavad tehnilised meetmed. Moodsate tehniliste ja organisatsiooniliste meetmete rakendamine selleks, et kaitsta andmeid tuvastamise vastu, võib õigustada käsitust, et isik ei ole tuvastatav, võttes arvesse *kõiki vahendeid, mida vastutav töötleja või keegi muu võib tõenäoliselt kasutada* isikute tuvastamiseks. Sellisel juhul ei ole kõnealuste meetmete rakendamine direktiivi artiklist 17 tuleneva õigusliku kohustuse (mis kehtib üksnes isikuandmete puhul) tagajärg, vaid pigem *tingimus* selleks, et teavet ei käsitataks isikuandmetena ja selle töötlemisele ei kohaldataks direktiivi.

Varjunimega kaitstud andmed

Varjunime kasutamine on isikusamasuse varjamine. Selle eesmärk on koguda sama isiku kohta lisaandmeid, ilma et oleks vaja teada tema isikut. See on eriti asjakohane uuringutes ja statistikas.

Varjunime võib kasutada nii, et selle taga olevaid isikuid on võimalik tuvastada isikute ja nende varjunimede vastavusloendite või varjunime määramisel kahesuunaliste krüpteerimisalgoritmide abil. Isikut võib varjata ka nii, et isikusamasuse taastamine ei ole võimalik, näiteks ühesuunalise krüpteerimisega, millega luuakse üldjuhul anonüümsed andmed.

Varjunime kasutamise protsessi tõhusus sõltub paljudest teguritest (millises etapis varjunime kasutatakse, kui hästi on see kaitstud taastuvastamise eest, isikute arv, kelle seas isik varjub, võimalus seostada üksikuid tehinguid või dokumente sama isikuga jne). Varjunimed peaksid olema juhuslikult valitud ja ennustamatud. Võimalike varjunimede arv peaks olema võimalikult suur, et kunagi ei valitaks juhuslikult sama varjunime. Kui

on vajalik eriti kõrge turvalisus, peab võimalike varjunimede arv vähemalt võrduma turvaliste krüptograafiliste räsifunktsioonide väärtuse arvuga.¹³

Isiku taastuvastamist võimaldava varjunimega varustatud andmeid võib käsitada teabena *kaudselt tuvastatava* isiku kohta. Tõepoolest, varjunime kasutamine tähendab, et on võimalik jõuda tagasi isikuni, nii et on võimalik tuvastada tema isikusamasus, kuid ainult eelnevalt kindlaksmääratud asjaoludel. Kuigi sellisel juhul kohaldatakse andmekaitsemeetmeid, on sellise kaudselt tuvastatava teabe töötlemisel oht üksikisikutele enamasti väike, nii et kõnealuseid norme kohaldatakse põhjendatult paindlikumalt kui otseselt tuvastatavate isikute andmete töötlemise puhul.

Võtmega kodeeritud andmed

Võtmega kodeeritud andmed on klassikaline näide varjunime kasutamisest. Teave on seotud isikutega, kes on tähistatud koodiga, samas kui võtit, mis võimaldab koodi siduda isiku harilike tunnustega (näiteks nimi, sünnikuupäev, aadress), hoitakse eraldi.

Näide nr 17. Summeerimata statistilised andmed

Näitena, kui oluline on kõigi asjaoludega arvestamine selleks, et hinnata, kas tuvastamise vahendeid võidakse „tõenäoliselt” kasutada, võib tuua isikuandmed, mida töödeldakse riiklikes statistikaasutustes, kus teatud etapis hoitakse teavet summeerimata kujul ja see on seotud konkreetsete isikutega, kuid neile on nime asemel antud kood (näit isik koodiga X1234 joob klaasi veini rohkem kui kolm korda nädalas). Statistikaasutus hoiab koodide võtmeid eraldi (loetelu, milles koodid on seostatud isikute nimedega). Võib eeldada, et statistikaasutus võib kõnealust võtit „tõenäoliselt kasutada” ja seetõttu võib isikuga seotud teavet pidada isikuandmeteks ning asutus peab siinkohal järgima andmekaitsemeetmeid. Kujutlegem, et tarbijate veinijoomisharjumusi käsitlevad andmed edastatakse riigi veinitootjate organisatsioonile, et nad saaksid oma seisukohtade kaitsmisel toetuda statistikale. Selleks, et teha kindlaks, kas kõnealune andmete loetelu kujutab endast ikka veel isikuandmeid, tuleks hinnata, kas veinitarbijate isikut on võimalik tuvastada, „võttes arvesse kõiki vahendeid, mida vastutav töötleja või keegi muu võib tõenäoliselt kasutada”.

Kui kasutatud kood on iga konkreetse isiku puhul ainulaadne, esineb tuvastamise oht alati, kui on võimalik pääseda juurde krüpteerimisel kasutatud võtmele. Seetõttu tuleb otsustuses, kas *võttes arvesse kõiki vahendeid, mida vastutav töötleja või keegi muu võib tõenäoliselt kasutada*, on isikud tuvastatavad ja kas teavet tuleb seetõttu käsitada „isikuandmetena”, arvesse võtta selliseid tegureid nagu väljastpoolt sissehakkimise võimalus, samuti võimalus, et keegi saatja organisatsioonist annab hoolimata ametisaladuse hoidmise kohustusest võtme edasi, ja kaudse tuvastamise võimalikkus. Kui isikud on tuvastatavad, kohaldatakse andmekaitsemeetmeid. Erinev küsimus on see, et kõnealustes nõuetes võiks arvesse võtta, kas oht üksikisikule on vähenenud, ja kehtestada direktiivi sätetega võimaldatud paindlikkuse raames vähem või rohkem ranged töötlemise tingimused.

¹³ Vt Saksa föderaal- ja liidumaa andmekaitsevolinike andmekaitse tehniliste ja organisatsiooniliste tahkude komitee eraelu puutumatus suurendamise töörühma töödokument „Privacy-enhancing technologies” (oktoober 1997), avaldatud koduleheküljel:

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

Kui aga koodid ei ole ainulaadsed, vaid sama koodi (nt „123”) kasutatakse eri linnades asuvate isikute tähistamiseks ja eri aastate andmete puhul (eristades konkreetse isiku ainult aasta ja sama linna valimi piires), saaks vastutav töötleja või kolmas isik konkreetse isiku tuvastada üksnes siis, kui ta teaks, millist aastat ja millist linna andmed käsitlevad. Kui selline lisateave on kadunud ja ei ole tõenäoline, et seda saab taastada, võib otsustada, et teave ei viita tuvastatavale isikule ja selle suhtes ei kohaldata andmekaitseenõudeid.

Selliseid andmeid kasutatakse harilikult kliinilistes ravimiuuringutes. 4. aprilli 2001. aasta direktiiv 2001/20 liikmesriikide õigus- ja haldusnormide ühtlustamise kohta, mis käsitlevad hea kliinilise tava rakendamist inimtervishoius kasutatavate ravimite kliinilistes uuringutes¹⁴ sätestab kõnealuse tegevusala õigusliku raamistiku. Ravimeid katsetav arst/teadlane („uurija”) kogub teavet kliinilise uuringu tulemuste kohta iga patsiendi puhul eraldi, tähistades patsiendi koodiga. Uurija edastab teabe ravimitootjale või muudele asjaomastele isikutele („sponsorid”) ainult kodeeritud kujul, sest nad on huvitatud ainult biostatistilistest andmetest. Sellegipoolest hoiab uurija eraldi alles võtme, mille abil saab koodi seostada üldise teabega, et tuvastada patsiendid eraldi moel. Uurija on kohustatud nimetatud võtme alles hoidma, et kaitsta patsientide tervist juhul, kui ravimid osutuvad ohtlikuks, et patsiendid oleksid vajadusel tuvastatavad ning saaksid asjakohast ravi.

Tekib küsimus, kas kliinilistes uuringutes kasutatavaid andmeid saab käsitada andmetena „tuvastatava” füüsilise isiku kohta ja kas nende puhul tuleks seetõttu järgida andmekaitseenõudeid. Eespool kirjeldatud analüüsi kohaselt peab selleks, et otsustada, kas isik on tuvastatav, võtma arvesse kõiki vahendeid, mida vastutav töötleja või keegi muu võib tõenäoliselt kasutada kõnealuse isiku tuvastamiseks. Sellisel juhul on isikute tuvastamine (vajadusel asjakohase ravi osutamiseks) üks kodeeritud andmete töötlemise eesmärgi. Ravimitootja tõlgendab mõistet töötlemisvahendid, sh organisatsioonilised meetmed ja tema suhted uurijaga, kelle käes on võti, nii, et isikute tuvastamine ei ole üksnes midagi, mis *võib* toimuda, vaid pigem midagi, mis teatud asjaoludel *peab* toimuma. Seega kuulub patsiendi tuvastamine töötlemise eesmärkide ja vahendite hulka. Sellisel juhul võib järeldada, et kodeeritud andmed kujutavad endast teavet füüsilise isiku kohta, kes on tuvastatav kõikide isikute poolt, kes võivad olla võimaliku tuvastamisega seotud, ning siinkohal tuleks järgida andmekaitseenõudeid. See ei tähenda siiski, et mõni teine vastutav töötleja, kes töötleb sama kodeeritud andmete kogumit, tegeleks isikuandmete töötlemisega, kui vastavalt konkreetsele programmile, mille raames nimetatud muu vastutav töötleja tegutseb, on taastuvastamine sõnaselgelt välistatud ja selle tagamiseks rakendatakse asjakohaseid tehnilisi meetmeid.

Muudes uuringu- või sama projektiga seotud valdkondades võib andmesubjekti taastuvastamise välistada uuringuplaani ja asjaomase protsessi vastava kavandamisega, näiteks seeläbi, et välistatakse terapeutilised asjaolud. Tehnilistel ja muudel põhjustel võib olla siiski võimalik kindlaks teha, milliste inimeste kliiniliste andmetega on tegemist, kuid eeldatakse, et tuvastamist kunagi ei toimu ja selle ennetamiseks rakendatakse asjakohaseid tehnilisi meetmeid (nt krüptograafia, ühesuunaline räsimine). Isegi kui kõnealusest uuringuplaanist ja muudest meetmetest hoolimata võidakse teatud andmesubjektid tuvastada (ettenägematute asjaolude tõttu, näiteks andmesubjekti tunnuste juhusliku kokkusobitamise tõttu, mis paljastavad tema isikusamasuse), ei saa vastutava esmatöötleja poolt töödeldud teavet käsitada teabena

¹⁴ EÜT L 121, 1.5.2001, lk 34, ELT eriväljaanne 13/26, lk 299.

tuvastatud või tuvastatava isiku kohta, võttes arvesse *kõiki vahendeid, mida vastutav töötleja või keegi muu võib tõenäoliselt kasutada*. Seega ei kohaldata kõnealuste andmete töötlemisele direktiivi sätteid. Iseasi on, et tegelikult tuvastatavale teabele juurdepääsu saanud uue vastutava töötleja jaoks on kahtlemata tegemist „isikuandmetega”.

Programmiga Safe Harbour seotud korduma kippuv küsimus 14-7

Ravimiuuringute võtmega kodeeritud andmete küsimust on käsitletud programmi Safe Harbour raames.¹⁵ Korduma kippuv küsimus 14-7 on järgmine:

KKK 14 - Farmaatsia- ja meditsiinitooted

7. K: Uurimisandmed kodeeritakse alati päritolukohas põhiuurija poolt ainulaadse koodiga, et üksikute andmesubjektide identiteeti mitte paljastada. Selliste uuringute sponsoriteks olevad ravimitootjad selle koodi võtit ei saa. Ainulaadne koodi võti on ainult uurijal, et temal oleks võimalik uuritavaid eriolukordades tuvastada (nt kui on vajalik edaspidine meditsiiniline tähelepanu). Kas sellisel moel kodeeritud andmete edastamine EL-ist Ameerika Ühendriikidesse kujutab endast programmi Safe Harbour põhimõtete kohast isikuandmete edastamist?

7. V: Ei. See ei kujuta endast põhimõtete kohast isikuandmete edastamist.

Töörühma arvates ei lähe kõnealune programmi Safe Harbour raames esitatud väide vastuollu eespool toodud põhjendusega, mille kohaselt sellist teavet tuleb käsitada isikuandmetena, mille suhtes kohaldatakse direktiivi. Tegelikult ei ole KKK piisavalt täpne, sest selles pole öeldud, kellele ja millistel tingimustel andmed edastatakse. Töörühm leiab, et küsimus käsitleb juhtumit, kus võtmega kodeeritud andmed saadetakse vastuvõtjale USAs (näiteks ravimitootjale), kes saab ainult võtmega kodeeritud andmed ja ei saa kunagi teada, kes on patsiendid, sest seda teab ja saab teada, kui tekib vajadus ravi järele, ainult ELi arst/teadlane, kuid mitte USAs asuv ettevõtja.

Anonüümsed andmed

„Anonüümseid andmeid” direktiivi tähenduses võib määratleda kui teavet füüsilise isiku kohta, kui vastutav töötleja või mõni teine isik ei saa kõnealust isikut tuvastada, võttes arvesse *kõiki vahendeid, mida vastutav töötleja või keegi muu võib mõistlikkuse piires tõenäoliselt kasutada*. „Anonüümseks muudetud andmed” oleksid seega anonüümsed andmed, mis varem olid seotud tuvastatava isikuga, kuid mille puhul tuvastamine ei ole enam võimalik. Kõnealusele mõistele viidatakse ka 26. põhjenduses, milles on öeldud, et „kaitsmise põhimõtteid ei kohaldata teabe suhtes, mis on muudetud anonüümseks selliselt, et andmesubjekti ei ole enam võimalik tuvastada”. Jällegi sõltub hinnang sellele, kas andmed võimaldavad isikut tuvastada ja kas teavet saab pidada anonüümseks, konkreetsest olukorrast ning iga juhtumit tuleks analüüsida eraldi, pöörates erilist tähelepanu sellele, millises ulatuses võidakse mõistlikkuse piires vahendeid tuvastamiseks kasutada, nagu on kirjeldatud 26. põhjenduses. See puudutab eriti statistilisi andmeid, mille puhul hoolimata asjaolust, et teave võidakse esitada summeeritud andmetena, ei ole algvalim piisavalt suur ja muud andmed võivad teha isikute tuvastamise võimalikuks.

¹⁵ Komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ, EÜT L 215/7, 25.8.2000, lk 7, ELT eriväljaanne 16/01, lk 119.

Näide nr 18. Statistilised ülevaated ja hajutatud andmete kombineerimine

Lisaks üldisele andmekaitseõuete järgimise kohustusele eesmärgiga tagada statistiliste ülevaadete anonüümsus lasub statistikutel ametisaladuse hoidmise kohustus, ning seda reguleerivate normide kohaselt on neil keelatud avaldada andmeid, mis ei ole anonüümsed. See kohustab neid avaldama summeeritud statistilisi andmeid, mida ei ole võimalik kokku viia statistiliste andmete taga olevate tuvastatud isikutega. Kõnealune nõue on eriti asjakohane rahvaloenduse andmete avaldamisel. Igas olukorras tuleks määratleda künnis, millest allpool on võimalik asjaomaseid isikuid tuvastada. Kui tundub, et kriteeriumi tõttu on võimalik tuvastada isikud, kes kuuluvad teatud kategooriasse, ükskõik kui suur see ka pole (nt 6000 elanikuga linnas tegutseb ainult üks arst), tuleks sellisest „diskrimineerivast” kriteeriumist täielikult loobuda või lisada täiendavaid kriteeriume, mis „hajutavad” kõnealust isikut puudutavad andmed, et oleks tagatud statistilise saladuse hoidmine.

Näide nr 19. Videovalve salvestuste avaldamine

Kaupluse omanik paigaldab oma kauplusesse videovalvesüsteemi. Ta avaldab oma kaupluses videovalve abil tabatud varaste pildid. Pärast politsei sekkumist varjab ta varaste näod nende tumestamisega. Isegi pärast seda jääb siiski võimalus, et fotodel olevate isikute sõbrad, sugulased või naabrid tunnevad nad ära, sest näiteks kehakuju, soeng või rõivad on ikkagi äratuntavad.

4. NELJAS ELEMENT: „FÜÜSILINE ISIK”

Direktiiviga loodud kaitse puudutab füüsilisi isikuid, st inimesi. Seega on õigus isikuandmete kaitsele üldine õigus, mis ei piirdu teatava riigi kodanike või elanikega. Direktiivi teises põhjenduses on sõnaselgelt öeldud, et „andmetöötlussüsteemid on loodud selleks, et teenida inimkonda” ja et „füüsiliste isikute kodakondsusele ja elukohale vaatamata tuleb austada nende põhiõigusi ja -vabadusi”.

Füüsilise isiku mõistele on viidatud inimõiguste ülddeklaratsiooni artiklis 6, mille kohaselt „igal inimesel, ükskõik kus ta ka ei viibiks, on õigus oma õigussubjektsuse tunnustamisele”. Liikmesriikide õigusaktides, tavaliselt tsiviilõiguse valdkonnas, on täpsemalt sätestatud füüsilise isiku õigusvõime kui võime omada tsiviilõigusi ja kanda tsiviilkohustusi, mis algab isiku sünniga ja lõpeb tema surmaga. Seega on isikuandmed põhimõtteliselt andmed tuvastatud või tuvastatava *elusa inimese* kohta. See tekitab käesolevas analüüsis rida küsimusi.

Andmed surnud isikute kohta

Tuginedes eelnevale, ei käsitata teavet surnud isikute kohta põhimõtteliselt isikuandmetena direktiivi tähenduses, sest surnud ei ole enam füüsilised isikud tsiviilõiguse mõistes. Sellegipoolest võivad surnud isikuid käsitlevad andmed teatud kindlatel juhtudel kaudselt kuuluda kaitse alla.

Ühest küljest ei ole vastutaval töötlejal võimalik kindlaks teha, kas isik, kellega andmed on seotud, on veel elus või juba surnud. Või isegi kui ta seda teeb, võidakse surnuid käsitlevat teavet töödelda koos andmetega elavate kohta, tegemata nende vahel vahet. Kuna direktiiv kohustab vastutavaid töötlejaid kaitsma elavaid inimesi käsitlevaid andmeid, on surnuid käsitlevate andmete töötlemine samu

andmekaitseenõudeid järgides tegelikkuses ilmselt kergem, kui kahe andmekogumi eraldamine.

Teisest küljest võib surnud isikuid käsitlev teave viidata ka elavatele isikutele. Näiteks teave, et surnu Gaia põdes hemofiiliat, tähendab, et ka tema poeg Titius põeb sama haigust, kuna see antakse edasi x-kromosoomis asuva geeniga. Seega, kui surnut käsitlevad andmed on samal ajal seotud ka elavatega ja neid käsitatakse isikuandmetena, mis kuuluvad direktiivi reguleerimisalasse, võivad andmekaitseenõuded kaudselt laieneda andmetele surnud isiku kohta.

Kolmandaks võib surnut käsitlev teave kuuluda erikaitse alla, mis on andmekaitsealastest õigusaktidest sõltumata sätestatud teistes õigusaktides, mis sätestavad piirangud, mida mõnikord kutsutakse *personalitas praeterita*. Arstisaladuse hoidmise kohustus ei lõpe patsiendi surmaga. Isiku maine ja au kaitsmise õigust sisaldavas siseriiklikus õigusaktis võib olla sätestatud ka surnu mälestuse kaitse.

Neljandaks ei takista miski liikmesriike laiendamast siseriiklikke õigusakte, millega direktiiv 95/46/EÜ rakendatakse, valdkondadele, mis ei kuulu direktiivi kohaldamisalasse, kui ükski muu ühenduse õiguse säte seda ei välista, nagu on meenutanud Euroopa Kohus.¹⁶ On võimalik, et mõni liikmesriigi seadusandja võib otsustada laiendada siseriikliku andmekaitse seaduse sätteid surnud isikuid käsitlevate andmete töötlemise mõnedele tahkudele, kui seda põhjendab õiguspärane huvi.¹⁷

Sündimata lapsed

See, millises ulatuses kohaldatakse andmekaitseenõudeid enne sündi, sõltub siseriikliku õigussüsteemi üldisest seisukohast sündimata laste kaitsmise suhtes. Pidades peamiselt silmas pärimisõigust, tunnustavad mõned liikmesriigid põhimõtet, et eostatud, kuid veel sündimata lapsi käsitletakse hüvedega seoses sündinutena (ja nad võivad seega vastu võtta pärandi või annaku), seda tingimusel, et nad võivad tegelikult sündida. Teistes liikmesriikides on erikaitse samal tingimusel tagatud konkreetsete erinormidega. Selleks, et otsustada, kas siseriiklikud andmekaitsealased normid kaitsevad ka teavet sündimata laste kohta, tuleb arvesse võtta liikmesriigi õiguskorra üldist käsitlust koos põhimõttega, et andmekaitseenõuete eesmärk on isikute kaitse.

Teine küsimus kerkib seoses sellega, et asjaomasel õiguskorras valitsev üldine käsitlus lähtub eeldusest, et sündimata lastega seotud olukord piirdub raseduse ajaga. Selles ei võeta arvesse asjaolu, et näiteks külmutatud embrüote puhul võib olukord tegelikult kesta oluliselt kauem. Konkreetse õigusliku vastuse võib leida viljastamismeetodeid reguleerivatest erinormidest, mis käsitlevad embrüoid puudutava meditsiinilise ja geneetilise teabe kasutamist.

Juriidilised isikud

Kuna isikuandmete mõistes viidatakse üksikisikutele, st füüsilistele isikutele, ei hõlma direktiiv põhimõtteliselt teavet juriidiliste isikute kohta ja selles sätestatud kaitset neile

¹⁶ Euroopa Kohtu 6. novembri 2003. aasta otsus kohtuasjas C-101/2001: Lindqvist (EKL 2003, lk I-12971, lk 87, punkt 98).

¹⁷ Euroopa Liidu Nõukogu protokoll, 8.2.1995, dokument 4730/95: „Seoses artikli 2 punktiga a „kinnitavad komisjon ja nõukogu, et liikmesriigid sätestavad ise, kas ja mil määral käesolevat direktiivi kohaldatakse surnud isikute suhtes.”

ei kohaldata.¹⁸ Teatavad andmekaitseõuded võivad mitmesugustel asjaoludel sellegipoolest kaudselt kehtida ettevõtete või juriidiliste isikutega seotud teabe suhtes.

Eraelu puutumatus ja elektroonilist sidet käsitleva direktiivi 2002/58/EÜ mõned sätted laienevad juriidilistele isikutele. Selle artiklis 1 on sätestatud, et „2. Käesoleva direktiivi sätted täpsustavad ja täiendavad direktiivi 95/46/EÜ sätteid lõikes 1 nimetatud eesmärkidel. Lisaks sellele nähakse nende sätetega ette juriidilistest isikutest abonentide õigustatud huvide kaitse”. Samuti laiendavad artiklid 12 ja 13 abonentikatalooge ja pealesunnituid teavet käsitlevad sätted ka juriidilistele isikutele.

Lähtuvalt käesolevas dokumendis sätestatud kriteeriumidest võib teavet juriidilise isiku kohta objektiivsetel põhjustel käsitada ka teabena füüsilise isiku „kohta”. See on nii, kui juriidilise isiku nimi tuleneb füüsilise isiku nimest. Teiseks näiteks on ettevõtte elektronposti aadress, mida tavaliselt kasutab üks kindel töötaja, või teave väikeettevõtte kohta (mis õiguslikus käsitluses on pigem „objekt” kui juriidiline isik), mis võib kirjeldada omaniku käitumist. Kõikidel juhtudel, kui „sisu”, „eesmärgi” või „tulemuse” kriteerium võimaldab juriidilist isikut või ettevõtet käsitlevat teavet pidada teabeks füüsilise isiku „kohta”, tuleb seda käsitada isikuandmetena ning kohaldada andmekaitseõudeid.

Euroopa Kohus on selgitanud, et miski ei takista liikmesriike laiendamast direktiivi rakendavaid siseriiklike õigusakte valdkondadele, mis ei kuulu direktiivi reguleerimisalasse, kui ükski muu ühenduse õiguse säte seda ei välista.¹⁹ Seetõttu on mõned liikmesriigid, näiteks Itaalia, Austria ja Luksemburg, laiendanud vastavalt direktiivile vastu võetud siseriiklike seaduste mõningate sätete (näiteks turvameetmeid käsitlevate sätete) kohaldamist juriidiliste isikute andmete töötlemisele.

Nagu surnud isikuid käsitleva teabe puhul, nii võivad vastutavad töötajad praktilise töökorralduse tõttu juriidilist isikut käsitlevate andmete suhtes tegelikult rakendada andmekaitseõudeid. Kui vastutav töötaja kogub andmeid nii füüsiliste kui ka juriidiliste isikute kohta neid üksteisest eristamata ja koondab need ühte andmekogumisse, võivad andmetöötlusmehhanismid ja kontrollsüsteem olla üles ehitatud nii, et need vastavad andmekaitseõuetele. Tegelikult võib vastutava töötaja jaoks olla lihtsam kohaldada andmekaitsenorme igasuguse tema andmebaasides oleva teabe suhtes, kui püüda eristada füüsiliste ja juriidiliste isikute kohta käivaid andmeid.

¹⁸ Direktiivi 24. põhjendus: „käesolev direktiiv ei mõjuta õigusakte, mis käsitlevad juriidiliste isikute kaitset nende kohta käivate andmete töötlemisel”.

¹⁹ Euroopa Kohtu 6. novembri 2003. aasta otsus kohtuasjas C-101/2001: Lindqvist (EKL 2003, lk I-12971, lk 87, punkt 98).

IV. MIS JUHTUB, KUI ANDMED EI KUULU MÕISTE ALLA?

Nagu käesolevast arvamusest nähtub, võib erinevatel asjaoludel juhtuda, et teavet ei käsitata isikuandmetena. See on nii, kui andmeid ei kogutud füüsilise isiku kohta või kui isikut ei saa pidada tuvastatuks või tuvastatavaks. Kui töödeldavale teabele ei laiene „isikuandmete” mõiste, siis direktiivi ei kohaldata vastavalt selle artiklile 3. See ei tähenda siiski, et isikud jäetakse konkreetses olukorras ilma igasuguse kaitseta. Arvesse tuleb võtta järgmisi kaalutlusi.

Kui direktiiv ei ole kohaldatav, võidakse kohaldada siseriiklikku andmekaitseeadust. Artikli 34 kohaselt on direktiiv adresseeritud liikmesriikidele. Väljaspool direktiivi reguleerimisala ei kehti liikmesriikidele selles sätestatud kohustused, milleks on põhiliselt direktiivi järgimiseks vajalike siseriiklike õigus- ja haldusnormide jõustamine. Euroopa Kohus on siiski selgitanud, et miski ei takista liikmesriike laiendamast direktiivi rakendavaid siseriiklikke õigusakte valdkondadele, mis ei kuulu direktiivi reguleerimisalasse, kui ükski muu ühenduse õiguse säte seda ei välista. Seetõttu võib juhtuda, et teatud olukordades, mille puhul ei toimu direktiivis määratletud isikuandmete töötlemist, kohaldatakse siiski siseriiklikus õiguses ettenähtud kaitsemeetmeid. Näitena võib tuua võtmega kodeeritud andmed, sõltumata sellest, kas tegemist on isikuandmetega või mitte.

Kui andmekaitseõuded ei ole kohaldatavad, võivad teatavad tegevused siiski kujutada endast sekkumist Euroopa inimõiguste konventsiooni artikli 8 tähenduses, mis kaitseb õigust era- ja perekonnavalule, võttes arvesse Euroopa Inimõiguste Kohtu laiaulatuslikku praktikat. Teised õigusnormide kogumid, näiteks lepinguvälise kahju tekitamise õigus, karistusõigus või diskrimineerimisvastane õigus, võivad samuti pakkuda üksikisikutele kaitset olukorras, kus andmekaitsereegleid ei kohaldata, kuid kus mängus on erinevad õiguspärased huvid.

V. KOKKUVÕTE

Käesolevas arvamuses andis töörühm suuniseid direktiivis 95/46/EÜ ja sellega seotud ühenduse õigusaktides kasutatud isikuandmete mõiste käsitamise ja kohaldamise kohta eri olukordades.

Üldise seisukohana märgiti asjaolu, et Euroopa seadusandja tahe oli kehtestada isikuandmete lai mõiste, kuid see mõiste ei ole piiramatult. Alati tuleks meeles pidada, et direktiiviga kehtestatud õigusnormide eesmärk on kaitsta isikuandmete töötlemisel üksikisikute põhiõigusi ja -vabadusi, eeskätt nende õigust eraelu puutumatusse. Seetõttu tuleb kõnealuseid norme kohaldada olukordades, kus üksikisikute õigused võivad ohtu sattuda ja vajavad seepärast kaitset. Andmekaitseõuete kohaldamisala ei tohiks olla üleliia lai, kuid samuti tuleks hoiduda isikuandmete mõiste põhjendamatu kitsendamisest. Direktiivis on piiritletud selle reguleerimisala, jättes välja mitmed tegevusalad, samuti võimaldab direktiiv reeglite paindlikku kohaldamist selle reguleerimisalasse jäävate tegevusalade suhtes. Andmekaitseasutustel on oluline osa, leidmaks direktiivi kohaldamisel sobivat tasakaalu (vt II osa).

Töörühma analüüs põhines neljal peamisel elemendil, mida saab eristada mõiste „isikuandmed” määratluses: st „igasugune teave”, „tuvastatud või tuvastatav”, „füüsiline isik” ja „kohta”. Kõnealused elemendid on omavahel tihedalt seotud ja üksteisest sõltuvad, kuid määratlevad koos, kas andmeid tuleks käsitada „isikuandmetena”. Analüüsi toetavad näited EL-i liikmesriikide andmekaitseasutuste tegevusest.

- Esimene element – „igasugune teave” – nõuab mõiste avarat tõlgendamist, sõltumata teabe laadist või sisust ja selle esitamise tehnilisest vormingust. See tähendab, et nii objektiivne kui ka subjektiivne teave mis tahes isiku kohta võib kujutada endast „isikuandmeid”, sõltumata sellest, millisel andmekandjal see esitatakse. Arvamuses käsitletakse ka biomeetrilisi andmeid ja nende juriidilist eristamist inimkudede proovidest, millest andmed võivad pärineda (vt III osa punkt 1).
- Teine element – „kohta” – on seni jäänud sageli tähelepanuta, kuid on esmatahtis mõiste sisulise kohaldamisala määramisel, eriti seoses esemete ja uute tehnoloogiatega. Arvamuses on välja toodud kolm alternatiivset elementi (sisu, eesmärk ja tulemus), mille alusel tuleb otsustada, kas teave käib isiku „kohta”. See hõlmab ka teavet, mis võib kahtlemata mõjutada isiku kohtlemist või hindamist (vt III osa punkt 2).
- Kolmas element – „tuvastatud või tuvastatav” – keskendub tingimustele, mille alusel tuleks isikut käsitada „tuvastatavana”, eriti „vahendeid, mida vastutav töötaja või keegi muu võib tõenäoliselt kasutada” selle isiku tuvastamiseks. Kõnealuses analüüsis on oluline osa sellel, milline on konkreetse juhtumi taust ja asjaolud. Arvamuses käsitletakse ka „varjunimega kaitstud andmeid” ja „võtmega kodeeritud andmete” kasutamist statistilistes või ravimiuuringutes (vt III osa punkt 3).
- Neljas element – „füüsiline isik” – on seotud tingimusega, et „isikuandmed” puudutavad „elavaid inimesi”. Arvamuses arutletakse ka selle üle, kuidas käsitleda surnud isikute, sündimata laste ja juriidiliste isikute andmeid (vt III osa punkt 4).

Lõpetuseks vaatleb arvamus olukorda, kus andmed ei kuulu mõiste alla „isikuandmed”. Kõnealustel juhtudel pakutakse probleemide käsitlemiseks erinevaid lahendusi, sh direktiivi reguleerimisalasse mittekuuluvate siseriiklike õigusaktide kohaldamine tingimusel, et järgitakse ühenduse õigust (vt IV osa).

Töörühm kutsub kõiki huvitatud isikuid tutvuma põhjalikult käesolevas arvamus esitatud suunistega ja võtma neid arvesse siseriiklike õigusnormide tõlgendamisel ja kohaldamisel kooskõlas direktiiviga 95/46/EÜ.

Töörühma liikmed, kellest enamik on siseriiklikul tasandil järelevalvet teostavate andmekaitseasutuste esindajad, on võtnud endale kohustuseks arendada käesolevas arvamus esitatud suuniseid edasi oma pädevusvaldkonnas ja tagada siseriiklike õigusaktide nõuetekohane kohaldamine kooskõlas direktiiviga 95/46/EÜ.

Töörühm kavatseb käesolevas arvamus esitatud suuniseid kohaldada ja edasi arendada kõikjal, kus see on asjakohane, ja võtta neid hoolikalt arvesse oma tulevases töös, eriti seoses selliste teemadega nagu identifitseerimine e-valitsuse ja e-tervishoiu ning raadiosagedustuvastuse (RFID) kontekstis. Viimasega seoses kavatseb töörühm täiendavalt analüüsida seda, kuidas andmekaitseõuded võivad mõjutada raadiosagedustuvastuse kasutamist ja millised lisameetmed võivad osutada vajalikuks, et tagada andmekaitsega seotud õiguste ja huvide nõuetekohane austamine kõnealuses kontekstis.

Lõpetuseks soovib töörühm märkida, et teretulnud on igasugune tagasiside huvitatud isikutelt ja järelevalveasutustelt nende praktiliste kogemuste kohta arvamus esitatud suunistega, sh täiendavad näited lisaks käesolevas dokumendis toodutele. Töörühm kavatseb teemat aja jooksul uuesti arutada, et täiustada ühist arusaama isikuandmete

põhimõistest ja tagada direktiivi 95/46/EÜ ning sellega seotud ühenduse õigusaktide parem rakendamine ja ühetaoline kohaldamine.

Töörühma nimel

Peter SCHAAR
eesistuja