A 29. CIKK ALAPJÁN LÉTREHOZOTT ADATVÉDELMI MUNKACSOPORT

01248/07/HU
WP 136

4/2007 vélemény a személyes adat fogalmáról

Az elfogadás időpontja: június 20.

Ez a munkacsoport a 95/46/EK irányelv 29. cikke alapján jött létre. Független európai tanácsadó szerv adatvédelmi, valamint a magánélet tiszteletben tartásával kapcsolatos kérdésekben. Feladatait a 95/46/EK irányelv 30. cikke és a 2002/58/EK irányelv 15. cikke határozza meg.

A titkársági feladatokat ellátja: Európai Bizottság, a Jogérvényesülés, Szabadság és Biztonság Főigazgatósága, C.`Igazgatóság (Polgári igazságszolgáltatás, alapvető jogok és uniós polgárság), B-1049 Brüsszel, Belgium, LX-46 01/43. sz. iroda.

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

amely az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv[1] alapján jött létre,

tekintettel az említett irányelv 29. cikkére, 30. cikke (1) bekezdésének a) pontjára és (3) bekezdésére, valamint a 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv 15. cikke (3) bekezdésére,

tekintettel az EK-Szerződés 255. cikkére, valamint az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletre,

tekintettel a munkacsoport eljárási szabályzatára,

ELFOGADTA EZT A VÉLEMÉNYT:

[1] H L L 281., 1995.11.23., 31. o., elérhető az alábbi címen: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. BEVEZETÉS

A munkacsoport tisztában van azzal, hogy a személyes adatok fogalmát mélyreható elemzésnek kell alávetni. Az EU tagállamainak jelenlegi gyakorlatára vonatkozó információ arra enged következtetni, hogy a gyakorlat tekintetében van némi bizonytalanság és eltérés a tagállamok között e fogalom fontos vonatkozásai terén, ami a különféle összefüggésekben befolyásolhatja a meglévő adatvédelmi keretrendszer megfelelő működését. Az adatvédelmi szabályok alkalmazása és értelmezése központi elemének ezen elemzése mindenképpen nagy hatást gyakorol majd számos fontos kérdésre, és különös jelentősége lesz az olyan témakörökben, mint például a személyazonosság kezelése az e-kormányzat és az e-egészségügy, továbbá a rádiófrekvenciás azonosítás (RFID) területén.

A munkacsoport e véleményének célja, hogy közös értelmezést adjon a személyes adat fogalmának, azoknak a helyzeteknek, amelyekben a nemzeti adatvédelmi jogi szabályozást kell alkalmazni, valamint az alkalmazás módjának. A személyes adat fogalmának közös meghatározásán folyó munka egyenértékű annak meghatározásával, mi tartozik az adatvédelmi szabályok hatálya alá, és mi nem. E munka eredményeképpen a 29. cikk alapján létrehozott munkacsoport iránymutatást nyújt a nemzeti adatvédelmi szabályok alkalmazásához az Európa-szerte előforduló helyzetek egyes kategóriái vonatkozásában, és ezáltal járul hozzá alapvető feladatát ellátva az ilyen normák egységes alkalmazásához.

E dokumentum az elemzés alátámasztására és szemléltetésére olyan példákat dolgoz fel, amelyek az európai adatvédelmi hatóságok nemzeti gyakorlatában merültek fel. A legtöbb példa az e vonatkozásban való megfelelő felhasználás érdekében mindössze szerkesztésen ment át.

II. ÁLTALÁNOS SZEMPONTOK ÉS SZAKPOLITIKAI KÉRDÉSEK

Az irányelv a személyes adat tág fogalmát tartalmazza

A személyes adatnak a 95/46/EK irányelvben (a továbbiakban: az adatvédelmi irányelv vagy irányelv) található meghatározása a következőképpen hangzik:

„személyes adat" az azonosított vagy azonosítható természetes személyre („érintettre") vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén".

Meg kell jegyezni, hogy e fogalommeghatározás az európai jogalkotó azon szándékát tükrözi, hogy a „személyes adat" tágabb értelemben vett meghatározását adja, amelyet megtart a jogalkotási folyamat egésze során. A Bizottság eredeti javaslatában kifejti, hogy „*a 108. egyezménynek megfelelően tágabb értelemben vett fogalommeghatározást fogadtak el annak érdekében, hogy az kiterjedjen valamennyi, személyhez kapcsolható információra*"[2]. A Bizottság módosított javaslatában megjegyzi, hogy „*a módosított javaslat teljesíti a Parlament azon kérését, hogy a „személyes adat" fogalommeghatározása a lehető legáltalánosabb legyen, hogy ezáltal kiterjedjen az azonosítható személyt érintő valamennyi információra*"[3]; ezt a kérést a Tanács is figyelembe vette a közös állásfoglalás megalkotásánál[4].

Az irányelvben található szabályok célja az egyének védelme

A 95/46/EK és a 2002/58/EK irányelv 1. cikke egyértelműen meghatározza a benne foglalt szabályok végső célját: védeni a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében. Ez mindkét jogi eszköz szabályainak értelmezése és alkalmazása során olyan nagyon fontos elem, amelyet nem lehet figyelmen kívül hagyni. Lényegi szerepe lehet annak meghatározásában, ahogyan az irányelv rendelkezéseit számos olyan helyzetben alkalmazni kell, amikor az egyének jogai nincsenek veszélyben, és óvatosságra inthet ugyanazon szabályok bármely olyan értelmezésével szemben, amely révén az egyéneket megfosztanák jogaik védelmétől.

Az irányelv alkalmazásának hatálya számos tevékenységet kizár, és a szövegbe ágyazott rugalmasság megfelelő jogi választ kínál a kérdéses körülményekre

A „személyes adat" és a „feldolgozás" irányelvben található tágabb értelmű fogalma ellenére a puszta tény, hogy a meghatározás értelmében egyes helyzeteket „személyes adatok feldolgozását" is felölelőnek lehet tekinteni, nem jelenti önmagában azt, hogy ez a helyzet az irányelvben, különösen annak 3. cikkében foglalt szabályok hatálya alá

---

2 COM (90) 314 végleges, 1990.9.13., 19. o. (megjegyzés a 2. cikkhez).
3 COM (92) 422 végleges, 1992.10.28., 10. o. (megjegyzés a 2. cikkhez).
4 1/95/EK közös álláspont, amelyet a Tanács 1995. február 20-án fogadott el, HL C 93., 1995.4.13., 20. o.

tartozna. A közösségi jog alkalmazási köréből eredő mentességektől eltekintve, a 3. cikkben található mentességek figyelembe veszik a feldolgozás technikai módját (strukturálatlanul, manuálisan) és a felhasználás célját (természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozás). Még ahol a személyes adatok feldolgozására az irányelv hatálya alatt kerül is sor, nem feltétlenül kell a benne foglalt valamennyi szabályt az adott esetre alkalmazni. Az irányelv számos rendelkezése jelentős mértékben rugalmas, hogy ezáltal megfelelő egyensúlyt teremtsen egyrészről az érintett személy jogainak védelme, másrészről pedig az adatkezelő és harmadik személyek jogos érdeke, továbbá a közérdek között, amely szintén jelen lehet. Az ilyen rendelkezésekre – a teljesség igénye nélkül – példa található a 6. cikkben (az adat szükségességétől függő tárolási idő), a 7. cikk f) pontjában (érdekegyensúly a feldolgozás szükségességének igazolására), a 10. cikk c) pontjának utolsó bekezdésében és a 11. cikk (1) bekezdésének c) pontjában (szükség esetén az érintett tájékoztatása a tisztességes adatfeldolgozás biztosításához) és a 18. cikkben (az értesítési kötelezettség alóli mentesség).

Az adatvédelmi szabályok hatályát nem szabad túlfeszíteni

Nem kívánt eredményhez vezetne, ha adatvédelmi szabályokat olyan helyzetekre alkalmaznának, amelyeket e szabályok nem hivatottak lefedni, és amelyeket a jogalkotó nem kívánt e szabályok hatálya alá vonni. Az irányelv fent említett, 3. cikke szerinti lényeges mentességek és a (26) és (27) preambulumbekezdés értelmezései magyarázzák, hogyan kívánta a jogalkotó az adatvédelmet az alkalmazásban látni.

Az adatfeldolgozás módját egy korlátozás érinti. Érdemes emlékeztetni arra, hogy az első adatvédelmi jogszabályok hetvenes évekbeli elrendelése abból a tényből fakadt, hogy az elektronikus adatfeldolgozás formájában megvalósuló új technológia könnyebb és szélesebb körű hozzáférést biztosított a személyes adatokhoz, mint az adatkezelés hagyományos formái. Következésképpen az irányelv szerinti adatvédelem célja a feldolgozás azon formáinak védelme, amelyek tipikusan a személyes adatokhoz való könnyű hozzáférés nagyobb kockázatát jelentik ((27) preambulumbekezdés). Személyes adatok nem automatizált módon való feldolgozására az irányelvet csak azon adatoknál kell alkalmazni, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni (3. cikk).

Az irányelv szerinti adatvédelem alkalmazásának másik általános korlátozása az adatok olyan körülmények közötti feldolgozása, ahol az érintett azonosítására szolgáló eszközöket valószínűleg nem használnák fel ((26) preambulumbekezdés) – ezt a kérdést a későbbiekben megvizsgáljuk.

Kerülni kell a személyes adat fogalma értelmezésének indokolatlan korlátozását is

Azokban az esetekben, ahol az irányelv minden egyes rendelkezésének gépies alkalmazása első pillantásra rendkívül megterhelő vagy akár képtelen következményekkel járna, először is ellenőrizni kell, 1) hogy az adott helyzet az irányelv hatálya alá tartozik-e, különösen hogy megfelel-e az irányelv 3. cikkének; továbbá 2) amennyiben a hatálya alá tartozik, maga az irányelv vagy az annak megfelelően elfogadott nemzeti jogszabály nem engedélyez-e mentességet vagy egyszerűsítést egyes helyzetekre annak érdekében, hogy megfelelő jogi választ lehessen adni mindamellett, hogy védik az egyén jogait és a szóban forgó érdekeket. Helyesebb indokolatlanul nem korlátozni a személyes adat fogalommeghatározásának

értelmezését, hanem inkább azt szem előtt tartani, hogy jelentős a rugalmasság az adatokra vonatkozó szabályok alkalmazásánál.

A nemzeti adatvédelmi felügyelő hatóságok e tekintetben lényegi szerepet játszanak az adatvédelmi jogszabályok alkalmazását megfigyelő küldetéseik keretein belül, ami felöleli a jogi rendelkezések értelmezését, valamint az adatkezelőknek és az érintett személyeknek nyújtott konkrét iránymutatást. Helyben kell hagyniuk egy olyan fogalommeghatározást, amely elég tág ahhoz, hogy számoljon a fejlődéssel, és hatálya alá vonjon minden „homályos területet" mindamellett, hogy az irányelvben található rugalmasságot jogszerűen alkalmazza. Tulajdonképpen az irányelv szövege olyan szakpolitika kialakítására hív fel, amely egyesíti a személyes adat fogalmának tág értelmezését, valamint megfelelő egyensúlyt teremt az irányelv szabályainak alkalmazása terén.

III. A „SZEMÉLYES ADAT" FOGALOMMEGHATÁROZÁSÁNAK ELEMZÉSE AZ ADATVÉDELMI IRÁNYELVNEK MEGFELELŐEN

Az irányelvben található fogalommeghatározás négy fő alkotóelemből áll, amelyeket e dokumentum céljából elkülönítve elemzünk majd. Ezek a következők:

– „bármely információ",

– „vonatkozó",

– „azonosított vagy azonosítható",

– „természetes személy".

E négy alkotóelem szorosan egybefonódik, és kölcsönösen erősíti egymást. Az e dokumentumban követni kívánt módszer kedvéért azonban e fordulatokat egymástól elkülönítve kezeljük majd.

1. AZ ELSŐ ELEM: „BÁRMELY INFORMÁCIÓ"

Az irányelvben található „bármely információ" fordulat egyértelműen jelzi a jogalkotó szándékát a személyes adat tág értelmű fogalmának megalkotására. E megfogalmazás széles körű értelmezést kíván.

Az információ természetének szempontjából a személyes adat fogalommeghatározása a személyre vonatkozó állítások valamennyi fajtáját felöleli. Lefed „objektív" információkat, mint például egy adott anyag előfordulását valaki vérében. Tartalmaz továbbá „szubjektív" információt is, véleményt vagy értékelést. Az állítások ezen utóbbi fajtája a személyes adatok feldolgozásának tekintélyes részét teszi ki a bankihoz hasonló ágazatokban, például a hitelkérelmezők megbízhatóságának értékelése terén („Titiusz megbízható hitelfelvevő."), biztosításoknál („Titiusz várhatóan nem fog hamarosan meghalni.") vagy a foglalkoztatásnál („Titiusz jó munkavállaló és megérdemli az előléptetést.").

Ahhoz, hogy az információ „személyes adatnak" minősüljön, nem kell igaznak vagy igazoltnak lennie. Valójában az adatvédelmi szabályok már számolnak annak lehetőségével, hogy az információ nem helyes, továbbá biztosítják az érintett számára

az információhoz való hozzáférés jogát, valamint hogy megfelelő jogorvoslat[5] útján kifogásolhassa azt.

Az információ tartalma szempontjából a személyes adat fogalma valamennyi, információt tartalmazó adatra kiterjed. Ez lefedi természetesen azt a személyes információt is, amelyet különösen kockázatos jellege miatt az irányelv 8. cikkében leírt „szenzitív adatnak" kell tekinteni, de azon túl lefedi a sokkal általánosabb információtípusokat is. A „személyes adat" megnevezésbe beleértjük az egyén „szoros értelemben vett" magán- és családi életét érintő információkat is, de az olyan információt is, amely az egyén által végzett bármiféle, például a munkakörülményeivel vagy gazdasági, illetve társas viselkedésével kapcsolatos tevékenységekre vonatkozik. Ide tartoznak tehát az egyénekre vonatkozó információk, tekintet nélkül e személyek helyzetére vagy képességeire (mint fogyasztó, beteg, alkalmazott, ügyfél stb.).

1. példa: Foglalkozással kapcsolatos szokások és gyakorlatok

Gyógyszerek felírására vonatkozó információt (pl. gyógyszer törzskönyvi száma, gyógyszer neve, gyógyszer erőssége, gyártó, értékesítési ár, új vagy utántöltő csomagolás, alkalmazás indoka, generikus gyógyszert kizáró vény kibocsátásának indoka, gyógyszert felíró orvos családi és utóneve, telefonszám stb.), akár egyetlen vény vagy több vény alapján felismerhető sablonrecept formájában, az adott gyógyszert felíró orvosra vonatkozó személyes adatnak lehet tekinteni, még ha a beteg neve ismeretlen is. Így az azonosított vagy azonosítható orvosok által felírt vényekre vonatkozó információ átadása a vényköteles gyógyszerek gyártóinak személyes adatok harmadik személlyel történő közlését valósítja meg az irányelv értelmében.

Ezt az értelmezést az irányelv megfogalmazása maga is alátámasztja. Egyrészről úgy kell tekinteni, hogy a magán- és családi élet fogalma tág, ahogyan azt az Emberi Jogok Európai Bírósága is tisztázta[6]. Másrészről a személyes adatok védelmére vonatkozó szabályok meghaladják a magán- és családi élet tiszteletben tartásához való jog tágabb értelemben vett védelmét. Meg kell jegyezni, hogy az Európai Unió Alapjogi Chartája a 8. cikkben a személyes adatok védelméhez való jogot autonóm jogként rögzíti, amely elkülönül és eltér a 7. cikkben említett, a magánélethez való jogtól, és ugyanez a helyzet nemzeti szinten néhány tagállamban is. Ez megfelel az irányelv 1. cikke (1) bekezdése megfogalmazásának is, amelynek célja védeni „a természetes személyek alapvető jogait és szabadságait, *különösen* [de nem kizárólagosan] a magánélet tiszteletben tartásához való jogukat". Ennek megfelelően az irányelv külön utalást tesz az otthoni és családi élet körén kívül eső személyes adatok feldolgozására, mint például a munkajog (8. cikk (2) bekezdés b) pontja), a büntetőítéletek, a közigazgatási szankciók vagy a polgári ügyekben hozott határozatok (8. cikk (5) bekezdés) vagy a

[5] A helyesbítésre a helytelen állításnak ellentmondó állásfoglalással, vagy pedig a megfelelő jogorvoslati kérelem, például panasz benyújtásával kerülhetne sor.

[6] Az Emberi Jogok Európai Bíróságának az Amann kontra Svájc ügyben 2000. február 16-án hozott ítéletének 65. pontja: „[…] a „magánélet" fogalmát nem szabad megszorítóan értelmezni. A magánélethez való jog magában foglalja különösen a többi emberi lényhez fűződő kapcsolatok kialakításához és kibontakoztatásához való jogot; nincs továbbá elvi ok annak igazolására, hogy a szakmai vagy gazdasági jellegű tevékenységeket kizárjuk a „magánélet" fogalmából (lásd a Niemietz kontra Németország ügyben 1992. december 16-án hozott ítéletet (A sorozat 251-B, 33–34. o., 29. pont) és a fent említett Halford ítéletet, 1015–16. o., 42. pont). E tág értelmezés megfelel az Európa Tanács 1981. január 28-i egyezményében található értelmezésnek […]."

közvetlen üzletszerzés terén (14. cikk b) pont). Az Európai Bíróság[7] támogatta e tágabb értelmű megközelítést.

A forma vagy az információt tartalmazó adathordozó tekintetében a személyes adat fogalma lefedi az összes, bármiféle formában hozzáférhető információt, legyen az alfabetikus, numerikus, grafikus, képi vagy akusztikus. Ide tartozik a papíron, továbbá a számítógépes memóriában bináris kóddal, vagy például a videoszalagon tárolt információ is. Ez logikus következménye annak, hogy az irányelv hatálya kiterjed a személyes adatok automatikus feldolgozására is. Ebből a nézőpontból különösen a hang- és képadatok minősülnek személyes adatnak, amennyiben egyénre vonatkozó információt hordoznak. E tekintetben az irányelv 33. cikkében a hang- és képadatokra tett külön utalást annak megerősítéseként és tisztázásaként kell értelmezni, hogy ez a fajta adat ténylegesen az irányelv hatálya alá esik (feltéve, hogy valamennyi egyéb feltétel is megvalósul), és hogy rájuk az irányelvet alkalmazni kell. Valójában logikus ezt feltételezni az említett cikkben található rendelkezés kapcsán, amely értékelni próbálja, vajon az irányelv szabályai megfelelő jogi választ adnak-e ezeken a területeken. Ezt tovább magyarázza a (14) preambulumbekezdés, amely kimondja, hogy „*a természetes személyek hang- és képadatainak felvételére, továbbítására, feldolgozására, rögzítésére, tárolására és közlésére használatos módszereknek az információs társadalom keretén belül történő fejlesztésének fontosságát figyelembe véve ennek az irányelvnek alkalmazhatónak kell lennie az ilyen adatokhoz kapcsolódó feldolgozásra*”. Másrészről az információnak nem kell strukturált adatbázisban vagy -állományban lennie ahhoz, hogy személyes adatnak kelljen tekinteni. Elektronikus szabad szövegben található információ is minősülhet személyes adatnak, amennyiben a személyes adat fogalommeghatározásának többi feltétele teljesül. Az e-mail például tartalmaz „személyes adatot”.

2. példa: Telebank szolgáltatások

A telebank szolgáltatásoknál, ahol a banknak adott utasítások során az ügyfél hangját szalagon rögzítik, ezeket a rögzített utasításokat személyes adatnak kell tekinteni.

3. példa: Videokamerás megfigyelés

Az egyénekről videokamerás megfigyelőrendszerrel felvett képek személyes adatok lehetnek, amennyiben rajtuk az egyének felismerhetők.

4. példa: Gyermekrajzok

Gyermekelhelyezési perben benyújtottak egy kislány által a neuropszichiátriai vizsgálat során a családjáról készített rajzot. A rajz információval szolgált a kislány kedélyállapotáról és a család különböző tagjai iránti érzéseiről. E rajzot is mint olyat „személyes adatnak” lehetne tekinteni. A rajz tulajdonképpen információt tár fel a gyermekkel kapcsolatban (egészségi állapot pszichiátriai szempontból), valamint pl. az

[7] Az Európai Bíróságnak a C-101/01. sz. Lindqvist-ügyben 2003. november 6-án hozott ítéletének 24. pontja: „A személyes adatnak a 95/46 irányelv 3. cikkének (1) bekezdésében használt fogalma – az irányelv 2. cikkének a) pontjában található fogalommeghatározásnak megfelelően – az azonosított vagy azonosítható természetes személyre vonatkozó bármely információra kiterjed. E fogalom alá tartozik kétségkívül a személy nevének megadása is, amikor erre telefonos adataival vagy a munkakörülményeire, illetve a szabadidős tevékenységeire vonatkozó információval kapcsolatban kerül sor”.

apa vagy anya viselkedéséről is. Emiatt az esetben érintett szülők esetleg gyakorolhatják az ezen egyedi információhoz való hozzáféréshez való jogukat.

Külön utalást kell itt tennünk a biometrikus adatokra. Ezen adatokat meghatározhatjuk biológiai jellegzetességekként, pszichológiai sajátosságokként, életvitelként vagy olyan ismétlődő tevékenységekként, amelyek során e jellegzetességek és/vagy tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is. Az ilyen biometrikus adatok tipikus példáit adják az ujjlenyomatok, a retinaminták, az arcstruktúra, a hangok, de a kezek geometriája, az erezet mintázata vagy akár valamely mélyen rögzült képesség vagy egyéb viselkedési jellegzetesség is (mint például a kézi aláírás, a gépelés módja, a jellegzetes járás vagy beszéd stb.).

A biometrikus adatok egyik jellegzetessége, hogy egyaránt tekinthetők az adott egyénre vonatkozó információ *tartalmának* (ezek az ujjlenyomatok Titiusz ujjlenyomatai), valamint olyan elemnek, amely *kapcsolatot* teremt az adott információ és az egyén között (ezen a tárgyon valaki az érintésével hátrahagyta ezeket az ujjlenyomatokat, és ezek az ujjlenyomatok megfelelnek a Titiuszéinak; tehát ezt a tárgyat Titiusz érintette meg). Ilyetén módon ezek tehát „azonosítókként" működhetnek. Az adott egyénhez fűződő egyedi kapcsolódásuk révén a biometrikus adatokat csakugyan fel lehet használni az egyén azonosítására. E kettős jellegzetesség megjelenik a DNS-adatoknál is, amelyek információt nyújtanak az emberi testről, valamint lehetővé teszik a személy egyértelmű és egyedi azonosítását.

Az emberi szövetminták (mint például a vérminta) önmagukban olyan források, amelyekből biometrikus adatokat nyernek ki, de amelyek önmaguk nem biometrikus adatok (így például az ujjlenyomatminta biometrikus adat, de az ujj maga nem). Ennélfogva, amikor mintákból nyernek információt, az személyes adatok gyűjtésének minősül, amelyre az irányelvet alkalmazni kell. A szövetminták gyűjtése, tárolása és felhasználása különféle szabályrendszerek hatálya alá tartozhat[8].

2. A MÁSODIK ELEM: „VONATKOZÓ"

A fogalommeghatározás ezen építőeleme elengedhetetlen, hiszen nagyon fontos ahhoz, hogy pontosan megtaláljuk, melyek is azok a kapcsolatok/kapcsolódások, amelyek számítanak, valamint hogy hogyan kell köztük különbséget tennünk.

Általánosan fogalmazva az információt egyénre „vonatkozónak" tekinthetjük, ha az adott egyén*ről* szól.

Számos helyzetben ezt a kapcsolatot könnyen meg lehet teremteni. Például a személyügyi irodán az egyénről vezetett aktában nyilvántartott adatok egyértelműen az egyénnek mint alkalmazottnak a helyzetére „vonatkoznak". Ilyenek a beteg orvosi vizsgálatának eredményeire vonatkozó adatok is a kartotékban, illetve egy személy képe, amelyet a vele készített videointerjú során rögzítenek filmre.

Számos egyéb helyzetet lehet említeni, noha nem mindig olyan magától értetődő annak meghatározása, hogy az információ az adott egyénre „vonatkozik-e", mint az előző esetekben.

---

[8] Lásd az Európa Tanács Miniszteri Bizottságának a tagállamokhoz intézett, 2006. március 15-i Rec(2006)4 ajánlását az emberi eredetű biológiai anyagok kutatásáról.

Néhány esetben az adat által hordozott információ elsősorban tárgyakat, és nem egyéneket érint. Ezek a tárgyak rendszerint tartoznak valakihez, vagy pedig egyének által vagy egyénekre gyakorolt bizonyos hatásnak lehetnek kitéve, illetve jellemezheti őket egyénekhez vagy egyéb tárgyakhoz fűződő valamiféle fizikai vagy földrajzi közelség. Tehát csak közvetve merül fel a vélelem, hogy az információ ezekre az egyénekre vagy tárgyakra vonatkozik.

5. példa: Egy ház értéke

Egy adott ház értéke tárgyra vonatkozó információ. Az adatvédelmi szabályokat egyértelmű, hogy nem kell alkalmazni, amikor ezt az információt csak az adott kerület ingatlanárai szintjének szemléltetésére használják. Mindazonáltal, bizonyos körülmények között az ilyen információt személyes adatnak is kell tekinteni. Valójában a ház a tulajdonosának vagyontárgya, amelyet így például annak meghatározásához használnak fel, hogy a személy milyen mértékben köteles bizonyos adókat megfizetni. Ebben az összefüggésben vitathatatlan, hogy az ilyen információt személyes adatnak kell tekinteni.

Hasonló elemzést kell alkalmazni, amikor az adat elsősorban folyamatokra vagy eseményekre vonatkozik, például egy olyan gép működésére, amely során emberi közreműködésre van szükség. Bizonyos körülmények között ezt az információt szintén lehet egyénre „vonatkozó” információnak tekinteni.

6. példa: Autójavító műhely nyilvántartása

Az autószerelő vagy műhely által az autóról vezetett nyilvántartás információt tartalmaz az autóról, a kilométeróra állásáról, a műszaki ellenőrzések időpontjáról, a műszaki problémákról és az autó fizikai állapotáról. Ezek az információk a nyilvántartásban egy adott rendszámhoz és motorszámhoz vannak rendelve, amelyeket így a tulajdonossal lehet kapcsolatba hozni. Amikor számlázás céljából a műhely kapcsolatba hozza a járművet és tulajdonosát, az információ a tulajdonosra vagy a jármű vezetőjére „vonatkozik” majd. Ha a kapcsolatot az autót javító szerelővel hozzák létre a szerelő termelékenységének értékelése céljából, ez az információ a szerelőre is „vonatkozni” fog.

A munkacsoport már figyelmet fordított annak kérdésére, mikor is lehet az információt személyre „vonatkozónak” tekinteni. Az rádiófrekvenciás azonosító (RFID) címke miatt felmerülő adatvédelmi kérdésekről folytatott viták keretein belül a munkacsoport megjegyezte, hogy „*egyénre vonatkozik az adat, ha az egyén azonosságára, tulajdonságaira vagy viselkedésére utal, vagy ha az ilyen információt annak meghatározására vagy befolyásolására használják, ahogyan az adott személyt kezelik vagy értékelik.*[9]”

A fent említett esetek fényében, valamint az azonos irányvonalak mentén rá lehetne mutatni, hogy annak érdekében, hogy az adatot egyénre „vonatkozónak” lehessen tekinteni, „**tartalom**” elemnek, VAGY „**cél**” elemnek, VAGY pedig „**eredmény**” elemnek kell jelen lennie.

[9] A munkacsoport 105. számú dokumentuma: „Munkadokumentum az RFID-technológiával kapcsolatos adatvédelmi kérdésekről”, elfogadva 2005. január 19-én, 8. o.

A „**tartalom**” elem azokban az esetekben van jelen, ahol – a „vonatkozó” szó társadalmilag legegyértelműbb és általános értelmének megfelelően – az információt egy adott személyről adják meg, tekintet nélkül az adatkezelő vagy harmadik személy részéről fennálló bármiféle célra, vagy az információnak az érintettre gyakorolt hatására. Az információ akkor „vonatkozik” egy személyre, amikor az adott „személyről” szól, és ez az, amit az esetet övező valamennyi körülmény fényében értékelni kell. Például az orvosi vizsgálat eredményei egyértelműen a betegre vonatkoznak, vagy a vállalati nyilvántartásban az adott ügyfél neve alatt nyilvántartott információ egyértelműen ezen ügyfélre vonatkozik. Ugyanígy, az RFID-címkén vagy az adott személy személyazonossági okmányába épített vonalkódon tárolt információ az adott személyre vonatkozik, mint például a jövőbeli RFID-chipet tartalmazó útleveleknél.

A „**cél**” elem is felelős lehet azért a tényért, hogy az információ egy adott személyre „vonatkozzék”. E „cél” elemet meglévőnek lehet tekinteni, amikor az adatot az esetet övező valamennyi körülményt figyelembe véve abból a célból használják fel vagy használják fel valószínűleg, hogy az egyén státuszát vagy viselkedését értékeljék, bizonyos bánásmódban részesítsék vagy befolyásolják.

7. példa: Telefonos hívás-log

A vállalati irodában található telefon híváslogolása információval szolgál azokról a hívásokról, amelyeket egy adott vonalhoz csatlakoztatott telefonról indítottak. Ezen információt különféle alanyokkal lehet kapcsolatba hozni. Egyrészről a vonalat a vállalkozás számára tették elérhetővé, és a vállalkozás szerződéses kötelezettsége kifizetni ezeket a hívásokat. A telefonkészülék munkaidőben az adott alkalmazott ellenőrzése alatt áll, és a hívásokat feltételezhetően ő bonyolítja. A hívás-log információval szolgálhat a hívott személyről is. A telefont használhatja továbbá bármely olyan személy is, aki az alkalmazott távollétében a vállalkozás helyiségeiben tartózkodhat (pl. a takarító személyzet). Különböző célokból az adott telefonkészülék használatára vonatkozó információt kapcsolatba lehet hozni a vállalkozással, az alkalmazottal vagy a takarító személyzettel (például annak ellenőrzésére, mikor hagyta el a munkahelyet a takarító személyzet, amennyiben a vállalkozás helyiségeinek bezárása előtt telefonon jelenteniük kell, hogy mikor távoznak). Meg kell említeni, hogy a személyes adat fogalma itt mind a kimenő, mind pedig a bejövő hívásokra kiterjed, mivel valamennyi hívás tartalmaz az emberek magánéletére, társadalmi kapcsolataira és kommunikációjára vonatkozó információt.

A bizonyos személyekre „vonatkozás” harmadik fajtája akkor merül fel, amikor „**eredmény**” elem van jelen. A „tartalom” vagy a „cél” elem hiánya ellenére lehet adatot egyénre „vonatkozónak” tekinteni, amennyiben felhasználása valószínűleg hatással van egy adott személy jogaira és érdekeire, figyelembe véve az adott esetet övező valamennyi körülményt. Meg kell jegyezni, hogy a lehetséges eredménynek nem feltétlenül kell jelentős hatásnak lennie. Elégséges, ha az egyént az ilyen adatok feldolgozásának eredményeként a többiektől eltérő bánásmódban részesíthetik.

8. példa: Taxik helyzetének a szolgáltatás optimalizálásának érdekében történő figyelemmel kísérése, kihatással a gépjárművezetőkre

Egy taxi vállalat műholdas helyzetmeghatározó rendszert állított fel, amely lehetővé teszi a szabad taxik helyzetének valós idejű meghatározását. A feldolgozás célja jobb szolgáltatást nyújtani, valamint üzemanyagot megtakarítani azáltal, hogy a taxit rendelő egyes ügyfelekhez azt az autót küldik ki, amelyik az ügyfél címéhez a legközelebb található. Valójában a rendszerhez szükséges adat az autóra, és nem a gépjárművezetőre vonatkozik. A feldolgozás célja nem a gépjárművezetők teljesítményének értékelése, például útvonaluk optimalizálása révén. Mégis, a rendszer lehetővé teszi a gépjárművezető teljesítményének figyelemmel kísérését, és annak ellenőrzését, hogy betartja-e a sebességkorlátozásokat, megfelelő útvonalat választ-e, a volánnál ül-e, vagy pedig az autón kívül pihenőidőt tart stb. Ennek tehát jelentős hatása lehet az adott egyénekre, és mint olyat, ezen adatot természetes személyekre vonatkozónak is lehet tekinteni. A feldolgozást az adatvédelmi szabályok szerint kell végezni.

E három elemet (tartalom, cél, eredmény) vagylagos, nem pedig kumulatív feltételeknek kell tekinteni. Különösen, amikor a tartalomelem jelen van, akkor nincs szükség a többi elem meglétére ahhoz, hogy az információt az egyénre vonatkozónak tekintsük. Ennek folyománya, hogy ugyanazon információ egyidejűleg vonatkozhat különböző egyénekre attól függően, hogy az egyes személyek tekintetében melyik elem van jelen. Ugyanazon információ vonatkozhat Titiusz egyénre a „tartalom” elem

miatt (az adat egyértelműen Tituszról szól), ÉS Gaiuszra a „cél” elem miatt (fel fogják használni annak érdekében, hogy Gaiuszt bizonyos bánásmódban részesítsék), ÉS Sempronius az „eredmény” elem miatt (valószínűleg hatása van Sempronius jogaira és érdekeire). Ez azt is jelenti, hogy az adatnak nem kell valakire „irányulnia” ahhoz, hogy rá vonatkozónak lehessen tekinteni. Az előző elemzésből következően a kérdés, hogy az adat adott személyre vonatkozik-e, olyan kérdés, amelyet minden egyes adatelem esetén annak saját jellemzői alapján kell megválaszolni. Hasonlóképpen a tényt, hogy egy információ különféle személyekre vonatkozhat, szem előtt kell tartani az anyagi jogi rendelkezések alkalmazásánál (pl. a hozzáférési jog terjedelménél).

9. példa: Értekezlet jegyzőkönyvében foglalt információ

Annak szükségességére, hogy a fenti elemzést minden információra külön el kell végezni, ezen eset szolgál például, amelyben egy értekezletről készült jegyzőkönyvben található információkról van szó; a jegyzőkönyvvezető Sempronius rögzíti Titiusz, Gaiusz és Sempronius részvevők jelenlétét, a Titiusz és Gaiusz által tett kijelentéseket, valamint az egyes témákban történt előrelépéseket. Titiuszra vonatkozó személyes adatnak csak azt az információt tekinthetjük, hogy adott időben és helyen részt vett az értekezleten, és hogy bizonyos kijelentéseket tett. Gaiusznak a Sempronius által rögzített jelenléte az értekezleten, a kijelentései és az egy adott témában történt előrelépés NEM Titiuszra vonatkozó személyes adatok. Ez akkor is így van, ha az információ ugyanabban a dokumentumban található, és még ha éppen Titiusz volt is az, aki felvetette az értekezleten megvitatandó kérdést. Ennélfogva Titiusz, ha az információhoz való jogával az őt érintő személyes adatok tekintetében élni kíván, ez utóbbi információkról nem kaphat tájékoztatást. Azt, hogy ezen információ vajon Gaiusz és Sempronius személyes adatának tekinthető-e, és ha igen, milyen mértékben, elkülönítve kell meghatározni a fent leírt elemzés alkalmazásával.

3. A HARMADIK ELEM: „AZONOSÍTOTT VAGY AZONOSÍTHATÓ” [TERMÉSZETES SZEMÉLY]

Az irányelv alapján az információnak „azonosított vagy azonosítható” természetes személyre kell vonatkoznia. Ez a következő megfontolásokat veti fel.

Általában véve egy természetes személyt „azonosítottnak” tekinthetünk, ha személyek egy csoportján belül „elkülönül” a csoport valamennyi egyéb tagjától. Következésképpen a természetes személy akkor „azonosítható” – még ha az azonosításra eddig nem is került sor –, ha ennek megtétele lehetséges (ez a „-ható” képző jelentése). Így a gyakorlatban e második lehetőség az a küszöbfeltétel, amely meghatározza, hogy az információ a harmadik elem körébe tartozik-e.

Az azonosítást rendesen olyan különleges információk segítségével végzik, amelyeket „azonosítóknak” nevezhetünk, és amelyek különösen kiemelt és szoros kapcsolatban vannak az adott egyénnel. Példaként szolgálhatnak a személy megjelenésének külső jegyei, mint például a magassága, a hajszíne, a ruházata stb., vagy a személy olyan tulajdonsága, amelyet nem lehet azonnal érzékelni, mint például a hivatása, a funkciója, a neve stb. Az irányelv a „személyes adat” 2. cikkben található fogalommeghatározásában megemlíti ezeket az „azonosítókat”, amikor kimondja, hogy a természetes személy „*közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén*”.

„Közvetlen" vagy „közvetett módon" azonosítható

További értelmezés található a módosított bizottsági javaslat cikkeihez fűzött magyarázatban abban az értelemben, hogy „*adott személyt azonosítani lehet közvetlenül a neve, vagy közvetett módon a telefonszáma, autója rendszáma, társadalombiztosítási száma, útlevélszáma vagy olyan jellegzetes kritériumok kombinációja révén, amelyek alapján őt fel lehet ismerni azon csoport leszűkítésével, amelyhez tartozik (kor, foglalkozás, lakóhely stb.)*". Ezen állítás fordulatai egyértelműen jelzik, hogy annak mértéke, amennyire az azonosításhoz bizonyos azonosítókra szükség van, olyasvalami, ami az adott helyzet körülményeitől függ. Egy nagyon gyakori családnév nem elegendő valaki azonosításához – pl. hogy kiválasszák – egy ország teljes lakosságából, míg valószínűleg sikeres lesz az azonosítás egy osztály tanulói között. Még valamely kiegészítő információ – mint például „a fekete öltönyös férfi" fordulat – is azonosíthat valakit a közlekedési lámpánál álló gyalogosok között. Így tehát a kérdés, miszerint az egyén, akire az információ vonatkozik, azonosított-e, vagy sem, az eset körülményeitől függ.

A „közvetlen módon" azonosított vagy azonosítható személyek tekintetében a személy **neve** tulajdonképpen a legáltalánosabb azonosító, és a gyakorlatban az „azonosított személy" fogalma a személy nevére történő utalást majdnem mindig magában foglalja.

Az azonosság megállapítása érdekében a személy nevét néha össze kell kapcsolni egyéb információkkal (születési idő, szülők neve, cím vagy arckép), nehogy az illetőt összekeverjék az esetleges névrokonaival. Például az információt, miszerint Titiusz tartozik egy összeggel, azonosított személyre vonatkozónak lehet tekinteni, mivel egy személy nevével kapcsolódik össze. A név olyan információ, amely megmutatja, hogy az egyén a betűk és hangok mely kombinációját használja saját maga megkülönböztetésére, valamint arra, hogy őt másoktól meg tudják különböztetni azok a személyek, akikkel ő kapcsolatba lép. A név továbbá kiindulópont is lehet azon információ irányában, hogy hol is lakik az érintett személy, vagy éppen hol található, információval szolgálhat továbbá a családtagjairól (a családi név révén), valamint számos különféle jogi és társadalmi kapcsolatról, amelyek az adott névvel kapcsolatosak (iskolai pályafutás, orvosi kartotékok, bankszámlák). Akár a személy megjelenése is ismert lehet, ha a nevéhez egy róla készült képet is mellékelnek. A névhez kapcsolt mindezen új információk lehetővé tehetik valaki számára, hogy rákeressen a hús és vér egyénre, így az azonosítók révén az eredeti információ összekapcsolódik egy természetes személlyel, akit a többi egyéntől megkülönböztethetünk.

A „közvetett módon" azonosított vagy azonosítható személyek tekintetében ez a kategória jellemzően az „egyedi kombinációk" jelenségére vonatkozik, legyenek azok akár kis-, akár nagyméretűek. Azokban az esetekben, ahol a hozzáférhető azonosítók kiterjedése első látásra nem teszi senki számára lehetővé az adott személy kiválasztását, attól még e személy „azonosítható" lehet, mivel az említett információ más információkkal összekapcsolva (ez utóbbi akár megvan az adatkezelőnél, akár nincs) az egyént másoktól megkülönböztethetővé teszi. Ez az a pont, ahol az irányelv pontosít „a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén". Némely tulajdonság annyira egyedi, hogy valakit mindenféle erőfeszítés nélkül azonosítani lehet („Spanyolország jelenlegi miniszterelnöke"), de a részletek kombinációja a kategóriák szintjén (korcsoport, regionális eredet stb.) is meglehetősen bizonyító erejű lehet adott körülmények között, különösen ha az embernek valamiféle kiegészítő

információkhoz is van hozzáférése. E jelenséget a statisztikusok – akik mindig nagyon igyekeznek a titoktartás megszegését elkerülni – már kiterjedt vizsgálatnak vetették alá.

10. példa: Töredékes információ a sajtóban

Információt közölnek egy korábbi bűnesetről, amelyet a múltban az emberek nagy figyelemmel kísértek. A jelenlegi sajtóanyagban nem tüntetik fel a hagyományos azonosítók egyikét sem, különösen nem az érintett személyek nevét vagy születési idejét.

Nem tűnik ésszerűtlenül nehéznek olyan további információkat szerezni, amelyek segítségével kitalálhatjuk, kik is a főként érintett személyek, pl. úgy, hogy fellapozunk néhány, az adott időszakban megjelent újságot. Következésképpen nem lehet teljesen kizárni, hogy valaki esetleg így tesz (például fellapozza a régi újságokat), és ily módon nevekhez és egyéb azonosítókhoz jut a példában említett személyekre vonatkozóan. Ennélfogva igazoltnak tűnik, hogy az adott példában található információt „azonosítható személyekre vonatkozó információnak", és mint ilyet, „személyes adatnak" tekintsük.

Ezen a ponton meg kell jegyezni, hogy míg a gyakorlatban a név alapján történő azonosítás fordul elő a leggyakrabban, a név maga nem szükségszerűen azonosít egy személyt minden esetben. Ez történhet, amikor egyéb „azonosítókat" használnak egy személy kiválasztására. Annak megelőzése érdekében, hogy két személyt összekeverjenek az adatállományban, a személyes adatokat nyilvántartó komputerizált adatállományok rendszerint egyedi azonosítót rendelnek a nyilvántartásba vett személyekhez. A világhálón a web forgalmát megfigyelő eszközök ugyanígy megkönnyítik egy adott számítógép, és mögötte felhasználója viselkedésének azonosítását. Lépésről lépésre áll tehát össze a kép azon egyén személyiségéről, akinek bizonyos döntéseket tulajdonítani lehet. Még akár az egyén nevének és címének lekérdezése nélkül is lehet a személyt kategorizálni társadalmi–gazdasági, pszichológiai, filozófiai vagy egyéb feltételek alapján, és bizonyos döntéseket neki tulajdonítani, mivel az egyén csatlakozási pontja (a számítógép) szűken értelmezve már nem feltétlenül kéri a személyazonosság megadását. Más szavakkal, az egyén azonosításának lehetősége többé már nem feltétlenül jelenti a neve megállapításának képességét. A személyes adat fogalommeghatározása tükrözi e tényt[10].

Az Európai Bíróság ilyen értelemben nyilatkozott, amikor úgy tekintette, hogy „*valamely internetes oldalon a különböző személyekre történő utalás, és nevük révén vagy egyéb módon, például a telefonszámukat, munkakörülményeiket vagy szabadidős tevékenységüket érintő információ megadásával történő azonosításuk személyes adatoknak a 95/46/EK irányelv értelmében vett [...] feldolgozásának minősül*"[11].

11. példa: Menedékkérők

A menedéket nyújtó intézményben valódi nevüket titokban tartó menedékkérők adminisztratív célokból kódszámot kapnak. Ez a szám azonosítóként szolgál, hogy a menedékkérőnek az említett intézményben való tartózkodását érintő különféle információkat ehhez rendeljék hozzá; fénykép vagy egyéb biometrikus mutatók

[10] Az Yves POULLET és mtsai által az Európa Tanács T-PD bizottsága számára készített, az adatvédelmi elveknek a világszerte alkalmazott távközlési hálózatokra való alkalmazásáról szóló jelentés, 2.3.1. pont, T-PD (2004) 04 végleges.

[11] Az Európai Bíróságnak a C-101/01. sz. Lindqvist-ügyben 2003. november 6-án hozott ítéletének 27. pontja.

segítségével a kódszám szoros és azonnali kapcsolatot teremt a valódi személlyel; ezáltal e személy megkülönböztethetővé válik a többi menedékkérőtől, hozzá továbbá különböző információkat lehet rendelni, amelyek akkor már egy „azonosított” természetes személyre utalnak majd.

A 8. cikk (7) bekezdése kimondja, hogy „[a] tagállamok határozzák meg a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek feldolgozásának feltételeit”. Érdemes figyelembe venni e rendelkezés értelmét, amely nem tartalmaz ugyan a tagállamok által elfogadandó feltételek típusára külön utalást, mégis a szenzitív adatokról szóló cikkbe került. A (33) preambulumbekezdés úgy utal az adatok e típusára, mint „*amelyek jellegüknél fogva sérthetik az alapvető szabadságokat vagy a magánéletet*”. Ésszerű a gondolat, hogy a jogalkotó hasonló aggodalmat érezhetett a nemzeti azonosító számok tekintetében, mivel erős a valószínűsége, hogy azok könnyen és visszavonhatatlanul összekapcsolhatnak az adott egyénre vonatkozó különféle információkat.

Az azonosítás eszközei

Az irányelv (26) preambulumbekezdése különös figyelmet szentel az „azonosítható” kifejezésnek, amikor kimondja, hogy „*mivel annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására*”. Ez azt jelenti, hogy az egyén kiválasztásának csupán hipotetikus lehetősége nem elég ahhoz, hogy a személyt „azonosíthatónak” tekintsük. Ha figyelembe véve „*minden olyan módszert ... amit az adatkezelő, vagy más személy valószínűleg felhasználna*”, e lehetőség nem létezik, vagy elhanyagolható, a személyt nem lehet „azonosíthatónak” tekinteni, és az információ nem számít „személyes adatnak”. A „*minden olyan módszer ... amit az adatkezelő, vagy más személy valószínűleg felhasználna*” feltételénél különösen figyelembe kell venni valamennyi szóban forgó tényezőt. Az azonosítás végrehajtásának költsége egy tényező, de nem az egyetlen. A szándékolt célt, a feldolgozás módjának strukturáltságát, az adatkezelő által várt előnyt, az egyének szóban forgó érdekeit, a szervezés működési zavarainak kockázatát (pl. a titoktartási kötelezettségek megsértése), valamint a műszaki meghibásodásokat mind-mind figyelembe kell venni. Másrészről itt egy dinamikus próbáról van szó, és tekintetbe kell venni a feldolgozás idején hozzáférhető csúcstechnológiát, valamint a fejlesztés lehetőségeit is azon időszak tekintetében, amelyre vonatkozóan az adatokat feldolgozzák. Meglehet, hogy ha a ma ésszerűen felhasználható összes módszert figyelembe is veszünk, az azonosítás jelenleg mégsem lehetséges. Ha az adatokat egy hónapig kívánják tárolni, az azonosítás lehetőségét esetleg nem is lehet elvárni ezen „élettartam” alatt, és az adatot nem is lehet személyes adatnak tekinteni. Mindazonáltal, ha ezen adatokat 10 évig akarják megtartani, az adatkezelőnek tudnia kell, hogy az azonosítás az adat élettartamának akár 9. évében is megtörténhet, és emiatt ezen adatok abban a pillanatban esetleg személyes adattá válhatnak. A rendszernek képesnek kell lennie ezen fejlődésekhez azok megtörténése ütemében alkalmazkodni, és alkalmas időben beépíteni a megfelelő technikai és szervezési intézkedéseket.

12. példa: Röntgenfelvételek közzététele a beteg keresztnevével

Egy hölgy röntgenfelvételét közzétették egy tudományos folyóiratban a hölgy keresztnevével együtt, amely azonban meglehetősen ritka név volt. A személy keresztneve, együttesen azzal, hogy rokonai és ismerősei tudtak arról, hogy egy

bizonyos betegségben szenved, számos személy számára azonosíthatóvá tette a személyt, ennélfogva a röntgenfelvételt tehát személyes adatnak kellene tekinteni.

13. példa: Gyógyszeripari kutatások adatai

Kórházak és egyéni orvosok betegeik kartotékaiból adatokat juttatnak el orvosi kutatás céljából egy vállalathoz. A betegek nevét nem használják, az egyes klinikai esetekhez csak véletlenszerűen rendelnek sorozatszámot annak érdekében, hogy biztosítsák az összefüggést, és elkerüljék a különböző betegekre vonatkozó információk összekeveredését. A betegek neve az adott orvos kizárólagos birtokában marad, őt pedig köti az orvosi titoktartás. Az adatok nem tartalmaznak semmiféle további olyan információt, amely összekapcsolás révén lehetővé tenné a betegek azonosítását. Továbbá valamennyi egyéb – jogi, technikai vagy szervezési jellegű – intézkedést megtettek, hogy megakadályozzák az érintettek azonosítását vagy azonosíthatóvá válását.
E körülmények között az adatvédelmi hatóság úgy tekintheti, hogy a gyógyszeripari vállalat által végzett feldolgozás során nem áll rendelkezésre olyan módszer, amelyet valószínűleg felhasználnának az érintettek azonosítására.

Amint fent említésre került, a „*minden olyan módszert ... amit ... valószínűleg felhasználna”* a személyek azonosításához fordulat értékelésénél lényeges tényezővé valójában az adatkezelő által az adatfeldolgozás során követett cél válik. A nemzeti adatvédelmi hatóságok olyan esetekkel találkoztak, ahol egyrészről az adatkezelő állítása szerint csak elszigetelt információt dolgoztak fel névre vagy bármely más közvetlen azonosítóra való utalás nélkül, valamint az ügyvédek szerint az adatokat nem kell személyes adatoknak tekinteni, és nem tartoznak az adatvédelmi szabályok hatálya alá. Másrészről az adott információ feldolgozásának csak akkor van értelme, ha lehetővé teszi az egyes személyek azonosítását, valamint hogy őket adott bánásmódban részesítsék. Ezekben az esetekben, ahol a feldolgozás célja magában hordozza az egyének azonosítását, feltételezni lehet, hogy az adatkezelőnek vagy bármely más, beavatott személynek megvannak vagy meglesznek azok a módszerei, amelyeket „valószínűleg felhasznál” majd az érintett azonosítására. Valójában azt állítani, hogy ezek az egyének nem azonosíthatók, amikor a feldolgozás célja pontosan az azonosításuk, önmagának teljesen ellentmondana. Ennélfogva az információkat azonosítható egyénekre vonatkozónak kell tekinteni, és feldolgozásuk az adatvédelmi szabályok hatálya alá tartozik.

14. példa: Videokamerás megfigyelés

Ez különösen jelentős a videokamerás megfigyelés vonatkozásában, ahol is az adatkezelők gyakran állítják, hogy azonosítás csak az összegyűjtött anyag kis százalékában történik meg, így aztán a ténylegesen megvalósuló néhány alkalommal történő azonosítás előtt személyes adatot nem dolgoznak fel. Mivel azonban a videokamerás megfigyelés célja minden esetben a videoképeken látható személyek azonosítása, amikor az ilyen azonosítást az adatkezelő szükségesnek tekinti, a teljes alkalmazást mint olyat azonosítható személyekre vonatkozó adatok feldolgozásának kell tekinteni, még ha egyes felvett személyek gyakorlatilag nem is azonosíthatók.

15. példa: Dinamikus IP-címek

A munkacsoport az IP-címeket már korábban azonosítható személyekre vonatkozó adatnak nyilvánította. Kijelentése szerint az „*internethozzáférést biztosító szolgáltatók*

és a helyi hálózatok kezelői ésszerű módszerek alkalmazásával azonosíthatják az általuk IP-címmel ellátott internetfelhasználókat, mivel rendes körülmények között szisztematikusan »beloggolják« egy fájlba a dátumot, az időt, az időtartamot és az internetfelhasználóhoz rendelt IP-címet. Ugyanezt lehet elmondani azon internetes szolgáltatókról is, akik a HTTP-szerveren logbookot vezetnek. Ezekben az esetekben nem kétséges, hogy az irányelv 2. cikkének a) pontja értelmében személyes adatról beszélhetünk."[12]

Különösen azokban az esetekben, ahol az IP-címek feldolgozását a számítógép felhasználójának azonosítása céljából végzik (például szerzői jogok birtokosai, hogy szellemi tulajdonjogok megsértése miatt számítógép-felhasználók ellen feljelentést tehessenek), mérlegeli előre az adatkezelő, hogy „minden olyan módszer ... amit ... valószínűleg felhasználna" a személyek azonosításához, az hozzáférhető pl. a feljelentés helye szerinti bíróságok révén is (egyébként az információgyűjtésnek nem lenne értelme); ennélfogva pedig az információt személyes adatnak kell tekinteni.

Sajátos lenne néhány olyan típusú IP-cím esete, amelyek bizonyos körülmények között valójában különféle technikai és szervezési okoknál fogva nem teszik lehetővé a felhasználó azonosítását. Erre példa lehetne az olyan internet kávézókban található számítógépekhez rendelt IP-cím, ahol a vendégnek nem kell igazolnia magát. Lehetne állítani, hogy az X számítógép használatáról egy adott időkeretben gyűjtött adatok nem teszik lehetővé a felhasználó ésszerű módszerekkel való azonosítását, és ennélfogva azok nem személyes adatok. Mindazonáltal meg kell jegyezni, hogy az internetes szolgáltatók nagy valószínűséggel nem fogják tudni, hogy a kérdéses IP-cím vajon azonosítást lehetővé tevő cím-e, vagy sem, és ugyanolyan módon fogják feldolgozni az említett IP-címhez rendelt adatokat is, ahogyan az olyan felhasználók IP-címeihez rendelt adatokkal teszik, akik megfelelően nyilvántartásba vannak véve és azonosíthatóak. Így aztán az internetes szolgáltatónak valamennyi IP-információt személyes adatként kell kezelnie, ha a biztonság talaján kíván maradni, kivéve ha olyan helyzetben van, hogy teljes bizonyossággal el tudja dönteni az adatról, hogy az nem azonosítható felhasználóra vonatkozik.

16. példa: Graffitivel okozott kár

Egy szállító vállalkozás személyszállító járműveit többször megrongálták graffitis firkálással. A vállalkozás nyilvántartást kezdett vezetni a kár körülményeiről, valamint a megrongált tárgyak képeivel és a graffiti készítője által hátrahagyott „tag"-ekkel vagy „aláírás"-sal kapcsolatos információkról, hogy ezáltal könnyebb legyen a károkat felmérni és a készítők ellen jogi követeléseket támasztani. Az információ nyilvántartásba vételének pillanatában a kárt okozó graffiti készítői nem ismertek, és az sem, hogy kinek felel meg az „aláírás". Könnyen meglehet, hogy soha nem is lesz az. Mindazonáltal az eljárás célja pontosan az olyan egyének azonosítása, akikre az információ mint a kárt okozó graffitik készítőire vonatkozik, hogy ezáltal jogi követeléseket lehessen velük szemben támasztani. Az ilyen eljárásnak akkor van értelme, ha az adatkezelő „valószínűnek" találja, hogy egy nap módja lesz azonosítani az egyént. A képeken található információt „azonosítható" egyénekre vonatkozónak, a nyilvántartásban található információt pedig „személyes adatnak" kell tekinteni, és a feldolgozást az adatvédelmi szabályok szerint kell folytatni, amelyek e feldolgozást

[12] WP 37: Titoktartás az Interneten – Az online adatvédelem integrált európai uniós megközelítése, elfogadva 2000. november 21-én.

jogszerűvé teszik adott körülmények között, továbbá megfelelő biztosítéki intézkedések megtételére köteleznek.

Amikor az érintett azonosítása nem szerepel a feldolgozás céljai között, az azonosítás megakadályozását célzó technikai intézkedések nagyon fontos szerepet játszanak. Az adatok azonosítás elleni védelme céljából életbe léptetett megfelelő csúcstechnológiával és szervezési intézkedésekkel elérhető, hogy a személyeket ne lehessen azonosíthatónak tekinteni, figyelembe véve minden olyan módszert, amelyet az adatkezelő vagy más személy valószínűleg felhasználna az említett személy azonosítására. Ebben az esetben ezen intézkedések végrehajtása nem az irányelv 17. cikkéből eredő jogi kötelezettség *következménye* (amely cikket csak akkor kell alkalmazni, ha az információ elsősorban személyes adat), hanem éppen inkább annak *feltétele*, hogy az információt ne kelljen személyes adatnak tekinteni, és feldolgozása ne essen az irányelv hatálya alá.

Pszeudonimmá tett adat

A pszeudonimizálás a személyazonosság elrejtésének folyamata. Az ilyen eljárás célja, hogy ugyanazon személyre vonatkozó további adatokat lehessen gyűjteni anélkül, hogy személyét meg kellene ismernünk. Ez különösen fontos a kutatás és a statisztikák terén.

A pszeudonimizálást el lehet végezni visszafelé követhető módon úgy, hogy a személyazonosságról és a pszeudonimekről megfeleltetési jegyzékeket vezetnek, vagy a pszeudonimizáláshoz kétutas kriptográfiai algoritmusokat alkalmaznak. A személyazonosságot oly módon is el lehet rejteni, hogy az újbóli azonosítás ne legyen lehetséges, például egyutas kriptográfiával, amely általában anonimizált adatokat hoz létre.

A pszeudonimizálási eljárás hatékonysága számos tényezőtől függ (hogy az eljárás melyik szakaszában alkalmazták, mennyire biztonságos a visszafelé történő nyomon követés ellen, mekkora a populáció, amelyben az egyént elrejtették, annak képessége, hogy az egyedi ügyleteket vagy bejegyzéseket ugyanazon személyhez lehessen kapcsolni stb.). A pszeudonimeknek véletlenszerűnek és előre ki nem találhatóknak kell lenniük. A lehetséges pszeudonimek számának olyan nagynak kell lennie, hogy ugyanazt a pszeudonimet ne lehessen véletlenül kétszer kiválasztani. Ha magas szintű biztonság megléte a követelmény, a lehetséges pszeudonimek készletének legalább akkorának kell lennie, mint a biztonságos kriptografikus tördelési funkciók értékköre[13].

A visszafelé követhető pszeudonimizált adatot olyan személyekre vonatkozó információnak tekinthetjük, akik *közvetve azonosíthatók*. Valójában a pszeudonim használata azt jelenti, hogy vissza lehet jutni az egyénhez oly módon, hogy az egyén személyazonossága felfedhetővé váljon, de csak előre meghatározott körülmények között. Ebben az esetben, noha alkalmazni kell az adatvédelmi szabályokat, az ilyen közvetett módon azonosítható információ feldolgozása tekintetében az egyént érintő fennálló kockázatok a legtöbb esetben olyan csekélyek, hogy e szabályok alkalmazása igazoltan rugalmasabb, mintha közvetlen módon azonosítható személyekre vonatkozó információkat dolgoznának fel.

[13] Lásd a német szövetségi és tartományi adatvédelmi biztosoknak az adatvédelem technikai és szervezési vonatkozásaival foglalkozó bizottsága titoktartást fokozó technológiákkal foglalkozó munkacsoportjának „Titoktartást fokozó technológiák” című munkadokumentumát (1997. október), amely a http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm címen jelent meg.

Kulccsal kódolt adatok

A kulccsal kódolt adatok a pszeudonimizálás klasszikus példái. Az információ azon egyénekre vonatkozik, akiket kóddal jelölnek, míg a kód és az egyének általános azonosítója (mint például a név, születési idő, cím) közötti megfelelést létrehozó kulcsot külön tárolják.

17. példa: Nem aggregált adatok statisztikai célokra

Hogy mennyire fontos az azonosításhoz „valószínűleg felhasználható" eszközök értékelésénél valamennyi körülményt figyelembe venni, jól szemlélteti ez a példa, amelyben a személyes adatok nemzeti statisztikai hivatal által történő feldolgozásáról van szó. Itt a feldolgozás egy adott szakaszában az információt nem aggregált formában tárolják, és ilyenkor meghatározott személyekre utalnak, akiket azonban nevük helyett egy kóddal jelölnek (pl. az X1234 kódjelű személy hetente háromnál többször iszik meg egy-egy pohár bort). A statisztikai intézet elkülönítve tárolja e kódok kulcsait (azaz a jegyzéket, amely a kódokat a személyek nevéhez kapcsolja). E kulcsot a statisztikai intézet által „valószínűleg használt" eszköznek, és így a személyekhez kapcsolt információkészletet személyes adatoknak tekinthetjük, amelyeket az intézetnek az adatvédelmi szabályok alkalmazásával kell kezelnie. Most képzeljük el, hogy a fogyasztók borivási szokásaira vonatkozó adatok jegyzékét átadják a nemzeti borászati szervezetnek annak érdekében, hogy azok hivatalos álláspontjukat statisztikai számadatokkal tudják alátámasztani. Annak meghatározásához, hogy az említett információjegyzék még mindig személyes adat-e, értékelni kell, vajon az egyes borfogyasztókat azonosítani lehet-e „*minden olyan módszert figyelembe ... [véve], amit az adatkezelő, vagy más személy valószínűleg felhasználna*".

Ha az egyes személyek esetében használt kódok egyediek, fennáll az azonosítás kockázata, amennyiben hozzá lehet jutni a kódoláshoz használt kulcshoz. Ennélfogva az illetéktelen külső behatolás kockázata, annak valószínűsége, hogy valaki az adatküldő szervezettől – annak szakmai titoktartása ellenére – kiszolgáltatná a kulcsot, *és* a közvetett azonosítás megvalósíthatósága olyan tényezők, amelyeket figyelembe kell venni annak meghatározásakor, hogy a személyeket azonosítani lehet-e „*minden olyan módszert figyelembe ... [véve], amit az adatkezelő, vagy más személy valószínűleg felhasználna*", és hogy ennélfogva az információt „személyes adatnak" kell-e tekinteni. Ha ez így van, az adatvédelmi szabályokat alkalmazni kell. Más kérdés, hogy ezek az adatvédelmi szabályok figyelembe vehetnék, ha az egyéneket érintő kockázatok lecsökkentek, továbbá a feldolgozást fokozottan vagy kevésbé szigorú feltételek alá rendelhetnék az irányelv szabályai által lehetővé tett rugalmasság alapján.

Ha – ezzel ellentétben – a kódok nem egyediek, hanem ugyanazt a kódszámot (pl. 123) használják különböző városokban élő egyének jelölésére és eltérő évekből származó adatokra (az adott egyént csak egy éven és az azonos városból gyűjtött mintán belül megkülönböztetve), az adatkezelő vagy harmadik személy egy adott személyt csak akkor tudna azonosítani, ha tudná, mely évre és mely városra utal az adat. Ha ez a kiegészítő információ elvész, és nem valószínű, hogy visszanyerhető, akkor úgy tekinthetjük, hogy az információ nem utal azonosítható személyekre, és nem esik az adatvédelmi szabályok hatálya alá.

Ezt a fajta adatot használják általánosan a gyógyszerek klinikai kipróbálásánál. A helyes klinikai gyakorlat bevezetéséről és a klinikai vizsgálatok végzéséről szóló, 2001. április 4-i 2001/20/EK irányelv[14] hozza létre a jogi keretet ezen tevékenységek végzése tekintetében. A gyógyszereket tesztelő egészségügyi szakember / kutató („vizsgáló") gyűjti össze a klinikai eredményekre vonatkozó információt minden egyes beteg esetében, akiket kóddal jelöl meg. A kutató az információt a gyógyszeripari vállalkozásnak vagy egyéb érintett feleknek („megbízók") csak ebben a kódolt formában adja meg, hiszen ez utóbbiakat csak a biostatisztikai információ érdekli. Mindazonáltal a vizsgáló elkülönítve tart egy kulcsot, amely e kódot hozzárendeli az általános információhoz, hogy ennek révén elkülönített módon tudja azonosítani a betegeket. A betegek egészségének védelme érdekében arra az esetre, ha kiderülne, hogy a gyógyszer veszélyes, a vizsgálónak meg kell tartania ezt a kulcsot, hogy az egyes betegeket szükség esetén azonosítani lehessen, és megfelelő kezelést kaphassanak.

A kérdés itt az, hogy a klinikai vizsgálathoz felhasznált adatokat „azonosítható" természetes személyre vonatkozóknak tekinthetjük-e, és ezáltal az adatvédelmi szabályok hatálya alá tartoznak-e. A fent ismertetett elemzés szerint egy személy azonosíthatóságának meghatározásához minden olyan módszert figyelembe kell venni, amelyet az adatkezelő vagy más személy valószínűleg felhasználna az említett személy azonosítására. Ebben az esetben az egyének azonosítása (hogy szükség esetén megkaphassák a megfelelő kezelést) a kulccsal kódolt adatok feldolgozásának egyik célja. A gyógyszeripari vállalkozás megteremtette a feldolgozás eszközeit, ideértve a szervezési intézkedéseket és a kutatóval való kapcsolatait, aki oly módon tárolja a kulcsot, hogy az egyének azonosítása bizonyos körülmények között ne csak megtörténhessen, hanem valóban meg is történjen. A betegek azonosítása tehát beágyazódik a feldolgozás céljai és eszközei közé. Ebben az esetben arra a következtetésre lehet jutni, hogy az ilyen, kulccsal kódolt adatok a lehetséges azonosításba esetlegesen bevont valamennyi fél által azonosítható természetes személyekre vonatkozó információkat hoznak létre, így tehát ezen adatoknak az adatvédelmi jogszabályok hatálya alá kell tartozniuk. Ez azonban mégsem jelenti azt, hogy az ugyanazon kódolt adatkészletet feldolgozó bármely más adatkezelő személyes adatot dolgozna fel, amennyiben a külön rendszerben, amelyben ezek az egyéb adatkezelők működnek, az újbóli azonosítás kifejezetten kizárt, és e tekintetben megfelelő technikai intézkedésekre került sor.

A kutatás vagy az ugyanazon projekt egyéb területein előfordulhat, hogy az érintett személyek újbóli azonosítását kizárták a vizsgálati tervek és az eljárás kialakítása során, például mivel az említett területeknek nincs terápiás vonzata. Technikai vagy egyéb okokból mégis lehet rá mód, hogy kiderüljön, melyik személynek felelnek meg az egyes klinikai adatok, de az azonosításra feltételezhetőleg vagy várhatóan semmilyen körülmények között nem kerül sor, és megfelelő technikai intézkedéseket (pl. kriptografikus, visszafordíthatatlan tördelés) léptettek életbe annak érdekében, hogy ennek előfordulását megelőzzék. Ebben az esetben, még ha az egyes érintettek azonosítása meg is történne az említett vizsgálati tervek és intézkedések ellenére (előre nem látható körülmények miatt, mint például az érintett tulajdonságainak véletlen egyezése, amely felfedi a személyazonosságát), az eredeti adatkezelő által feldolgozott információt akkor sem kellene azonosított vagy azonosítható személyekre vonatkozónak tekinteni, *figyelembe véve minden olyan módszert, amelyet az adatkezelő vagy más személy valószínűleg felhasználna*. Feldolgozása tehát nem esne az irányelv

[14] HL L 121., 2001.5.1., 34. o.

rendelkezéseinek hatálya alá. Ettől eltérő eset, amikor az új adatkezelő valóban hozzáférést kap az azonosítható információhoz: ezt ilyenkor kétségkívül „személyes adatnak" kell tekinteni.

14-7. GYFK a „biztonságos kikötő rendszerről"

A kulccsal kódolt adatok kérdésével a gyógyszeripari kutatások terén a „biztonságos kikötő rendszer"[15] foglalkozik. A 14-7. GYFK így szól:

14. GYFK – Gyógyszeripari és gyógyászati termékek

7. K: A kutatási adatokat a kutatás vezetője egyedülálló módon és megváltoztathatatlanul kódolta azok keletkezésekor, hogy az egyéni érintettek személyazonosságát ne lehessen megismerni. Az ilyen kutatást támogató gyógyszeripari vállalkozások nem kapják meg a kulcsot. Az egyedülálló kóddal csak a kutató rendelkezik, annak érdekében, hogy a különleges körülmények esetén (pl. ha utólagos orvosi ellenőrzésre van szükség) azonosíthassa a kutatási alanyt. Az ilyen módon kódolt adatok továbbítása az EU-ból az Egyesült Államokba a személyes adatok „biztonságos kikötő" elvek alá tartozó továbbítását képezi?

7. V: Nem, ez nem képezi személyes adatok olyan továbbítását, amelyre az elvek vonatkoznak.

A munkacsoport úgy véli, hogy a biztonságos kikötő rendszer ezen állítása nem mond ellent a fenti indoklásnak, amely az ilyen információt az irányelv hatálya alá tartozó személyes adatnak tekinti. Valójában ez a GYFK nem eléggé pontos, mivel nem mondja ki, kinek és milyen feltételek mellett továbbítják az adatokat. A munkacsoport értelmezése szerint a GYFK arra az esetre utal, amikor a kulccsal kódolt adatokat az USA-ban található olyan címzettnek küldik (például gyógyszeripari vállalkozásnak), amely csak kulccsal kódolt adatokat kap, és soha nem ismeri meg a betegek személyazonosságát; e személyazonosság ismertté akkor válik az EU-beli gyógyászati szakember / kutató, és sosem az USA-beli cég előtt, ha kezelésre van szükség.

Anonim adatok

Az irányelv értelmében az „anonim adatot" úgy lehet meghatározni, mint természetes személyre vonatkozó bármely információt, ahol is a személyt sem az adatkezelő, sem egyéb személy nem tudja azonosítani, *minden olyan módszert figyelembe véve, amit az adatkezelő vagy más személy valószínűleg felhasználna* az említett személy azonosítására. Az „anonimizált adat" tehát olyan anonim adat lenne, amely korábban azonosítható személyre vonatkozott, de amelynél az azonosítás többé már nem lehetséges. A (26) preambulumbekezdés erre a megközelítésre utal, amikor kimondja, hogy „*a védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható*". Megismételve tehát, annak értékelése, hogy az adat lehetővé teszi-e az egyén azonosítását, valamint hogy az információt anonimnak vagy nem anonimnak tekinthetjük-e, a körülményektől függ, és eseti elemzést kell végezni, külön utalással annak mértékére, amennyire valószínű, hogy a módszereket a (26) preambulumbekezdésben foglaltak szerint az azonosításra felhasználják. Ennek különös jelentősége van a statisztikai információk esetében, ahol annak ellenére, hogy az információt aggregált adatként állítják elő, az eredeti minta nem eléggé nagy, és egyéb információk lehetővé tehetik az egyén azonosítását.

[15] A Bizottság 2000.7.26-i 2000/520/EK határozata (HL L 215., 2000.8.25., 7. o.).

18. példa: Statisztikai kutatások és elszigetelt információ kombinálása

Az adatvédelmi szabályok tiszteletben tartására irányuló általános kötelezettségük mellett a statisztikusoknak a statisztikai kutatások anonimitásának biztosítása érdekében a szakmai titoktartás speciális kötelezettségének kell eleget tenniük, és e szabályok alapján tilos nem anonim adatot közzétenniük. Emiatt olyan aggregált statisztikai adatokat kell közzétenniük, amelyeket valószínűleg nem lehet a statisztikák mögött lévő, azonosított személyhez rendelni. E szabály különösen jelentős a népszámlálási adatok közzétételénél. Minden egyes helyzetben meg kell határozni azt a küszöbértéket, amely alatt lehetségesnek tekintik az érintett személyek azonosítását. Amennyiben úgy tűnik, hogy egy kritérium lehetővé teszi személyek egy adott kategóriájának azonosítását, legyen az bármilyen nagy (pl. egy 6000 lakosú városban csak egyetlen orvos műt), ezt a „diszkriminatív" kritériumot teljes mértékben ejteni kell, vagy egyéb kritériumokat kell hozzáadni, hogy „felhígítsák" az adott személyre vonatkozó eredményeket, és ezáltal megvalósulhasson a statisztikai titoktartás.

19. példa: Videokamerás megfigyelés nyilvánossá tétele

Egy bolttulajdonos videokamerás megfigyelőrendszert telepít a boltjába. Boltjában kiteszi azoknak a tolvajoknak a képét, akiket a videokamerás megfigyelőrendszer segítségével kapott el. Rendőrségi intézkedést követően elsötétítéssel kitakarja a tolvajok arcát. Mindazonáltal még e művelet után is fennáll a lehetősége, hogy a fényképeken látható személyeket barátaik, rokonaik vagy szomszédaik felismerjék amiatt, hogy pl. alakjuk, hajviseletük és ruhájuk még mindig felismerhető.

4. A NEGYEDIK ELEM: „TERMÉSZETES SZEMÉLY"

Az irányelv szabályai által nyújtott védelem természetes személyekre, vagyis emberi lényekre alkalmazandó. A személyes adatok védelméhez való jog ebben az értelemben egyetemes jog, amely nem korlátozódik egy adott ország állampolgáraira vagy lakóira. Az irányelv (2) preambulumbekezdése kifejezetten kitér erre, mondván „*az adatfeldolgozási rendszerek célja az emberek szolgálata*", és „*a természetes személyek nemzetiségétől és lakóhelyétől függetlenül tiszteletben kell tartaniuk e személyek alapvető jogait és szabadságait*".

A természetes személy fogalmát az Emberi Jogok Egyetemes Nyilatkozatának 6. cikke tartalmazza, amely szerint „*[m]indenkinek joga van ahhoz, hogy jogalanyiságát bárhol elismerjék*." A tagállamok jogrendszere, általában a polgári jog területén, ennél pontosabban határozza meg az emberi lény személyiségének fogalmát, amely alatt azt érti, hogy az egyén születésétől kezdve haláláig jogviszonyok alanya lehet. Ennélfogva a személyes adatok elviekben azonosított vagy azonosítható *élő személyekre* vonatkoznak. Ez elemzésünk céljait tekintve számos kérdést vet fel.

Elhunyt személyekre vonatkozó adatok

Az elhunytakra vonatkozó információkat tehát elvben nem tekinthetjük az irányelv szabályai alá tartozó személyes adatoknak, hiszen a holtak a polgári jog szerint többé nem természetes személyek. Mindazonáltal az elhunytra vonatkozó adatok bizonyos esetekben közvetve mégis élvezhetnek bizonyos védelmet.

Egyrészről az adatkezelő esetleg nincs olyan helyzetben, hogy megállapítsa, az adat által érintett személy még él-e, vagy esetleg már meghalt. Vagy ha mégis megteheti, az

elhunytra vonatkozó információt megkülönböztetés nélkül ugyanazon rendszerben is fel lehet dolgozni, mint az élőkre vonatkozóakat. Mivel az élő egyénekre vonatkozó adatok tekintetében az adatkezelőnek eleget kell tennie az irányelv által előírt adatvédelmi kötelezettségeknek, a gyakorlatban valószínűleg könnyebb lesz számára az elhunytakra vonatkozó adatokat is az adatvédelmi szabályok által meghatározott módon feldolgozni, mintsem elkülöníteni a két adatkészletet.

Másrészről az elhunyt személyekre vonatkozó információ élő személyekre is utalhat. Például az információ, miszerint az elhunyt Gaia vérzékeny volt, arra utal, hogy fia, Titiusz is ugyanebben a betegségben szenved, hiszen ez az X kromoszómán található génhez kapcsolódik. Így, amikor az olyan információt, amely az elhunytra vonatkozó adat, egyidejűleg az élőre is vonatkozó adatnak, valamint az irányelv hatálya alá tartozó személyes adatnak is tekinthetünk, az elhunyt személyes adata közvetve az adatvédelmi szabályok védelmét élvezheti.

Harmadsorban, az elhunyt személyekre vonatkozó információ különleges védelmet kaphat az adatvédelmi jogszabályokon kívül eső szabályrendszerek révén, amelyek meghúzzák az úgynevezett „*personalitas praeterita*" határvonalát. A kórházi személyzet titoktartási kötelezettsége nem ér véget a beteg halálával. A személy saját képmásához és az emberi méltósághoz való jogára vonatkozó nemzeti jog védelmet nyújthat az elhunytak emlékének is.

És negyedszer, semmi sem akadályozza meg a tagállamokat abban, hogy kiterjesszék a 95/46/EK irányelv rendelkezéseit végrehajtó nemzeti jogszabályok hatályát az irányelvben foglalt területeken túlra, hacsak a közösségi jog egyéb rendelkezése ezt eleve ki nem zárja, ahogyan erre az EB emlékeztetett[16]. Lehetséges, hogy valamely nemzeti jogalkotó úgy határoz, hogy kiterjeszti a nemzeti adatvédelmi jog rendelkezéseinek hatályát az elhunyt személyekre vonatkozó adatok feldolgozásának némely vonzataira is, amennyiben jogszerű érdek ezt igazolja[17].

Még meg nem született gyermekek

Az adatvédelmi szabályok születés előtti alkalmazandóságának mértéke a nemzeti jogrendszereknek a még meg nem született gyermekek védelmére vonatkozó általános álláspontjától függ. Ha főképpen az öröklési jogosultságokat vesszük figyelembe, néhány tagállam elismeri az elvet, miszerint a már megfogant, de még meg nem született gyermekeket megszületettnek kell tekinteni, amennyiben juttatásokról van szó (és így hozzájuthatnak örökséghez, vagy elfogadhatnak adományt), azzal a feltétellel, hogy ténylegesen meg fognak születni. Más tagállamokban különös védelmet élveznek bizonyos jogi rendelkezések révén, ugyanazon feltétel megléte mellett. Annak meghatározásához, hogy a nemzeti adatvédelmi rendelkezések védik-e a még meg nem született gyermekekre vonatkozó információt is, a nemzeti jogrendszer általános megközelítését kell figyelembe venni, együttesen azzal az eszmével, hogy az adatvédelmi szabályok célja az egyének védelme.

A második kérdést az a megfontolás veti fel, hogy a jogrendszer általános válasza azon elváráson alapul, hogy a még meg nem született gyermekek helyzete a terhesség

---

16 Az Európai Bíróságnak a C-101/2001. sz. Lindqvist-ügyben 2003. november 6-án hozott ítéletének 98. pontja.

17 Az Európai Unió Tanácsának jegyzőkönyve, 1995.2.8., 4730/95 dokumentum: „A 2. cikk a) pontjára „A Tanács és a Bizottság megerősíti, hogy a tagállamok feladata meghatározni, hogy az irányelvet az elhunyt személyekre alkalmazzák-e, és ha igen, milyen mértékben."

időszakára korlátozódik. Nem számol azzal a ténnyel, hogy ez a helyzet tulajdonképpen jelentősen tovább is tarthat, mint például a fagyasztott embriók esetében. Végezetül sajátos jogi válaszokkal találkozhatunk különösen a reprodukciós technikákra vonatkozó azon rendelkezések terén, amelyek az embriókra vonatkozó gyógyászati vagy genetikai információ felhasználását szabályozzák.

Jogi személyek

Mivel a személyes adat fogalommeghatározása egyénekre, azaz természetes személyekre utal, a jogi személyekre vonatkozó információkra elvben nem terjed ki az irányelv, és nem alkalmazandó rájuk az általa nyújtott védelem sem[18]. Mindazonáltal egyes adatvédelmi szabályokat számos helyzetben közvetve mégis lehet vállalkozásokra vagy jogi személyekre vonatkozó információkra is alkalmazni.

A 2002/58/EK e-adatvédelmi irányelv néhány rendelkezése kiterjed a jogi személyekre is. Az irányelv 1. cikke kimondja, hogy „*(2) Ennek az irányelvnek a rendelkezései az (1) bekezdésben említett célok érdekében pontosítják és kiegészítik a 95/46/EK irányelvet. Rendelkeznek továbbá a jogi személyiséggel rendelkező előfizetők jogos érdekeinek védelméről*.” Ennek megfelelően a 12. és 13. cikk az előfizetői névjegyzékeket és a nem kívánt tájékoztatást érintő némely rendelkezés alkalmazását kiterjeszti a jogi személyekre is.

A jogi személyekre vonatkozó információt természetes személyekre „vonatkozónak” is lehet tekinteni saját jellemzői alapján, az e dokumentumban meghatározott feltételeknek megfelelően. Ilyen eset lehet, amikor a jogi személy neve természetes személy nevéből származik. Másik példa lehet a vállalati e-mail, amelyet rendes körülmények között egy adott alkalmazott használ, vagy egy olyan kicsi vállalkozásra (jogi értelemben inkább „tárgyra”, mint jogi személyre) vonatkozó információ, amely jellemezheti tulajdonosának viselkedését. Mindezen esetekben, ahol a „tartalom”, a „cél” vagy az „eredmény” feltétele lehetővé teszi, hogy a jogi személyre vagy vállalkozásra vonatkozó információt természetes személyre „vonatkozónak” tekinthessük, az információt személyes adatnak kell tekinteni, és az adatvédelmi szabályokat alkalmazni kell.

Az Európai Bíróság egyértelművé tette, hogy semmi sem akadályozza meg a tagállamokat abban, hogy az irányelv rendelkezéseit végrehajtó nemzeti jogszabályaik hatályát kiterjesszék olyan területekre is, amelyek nem tartoznak az irányelv hatálya alá, amennyiben a közösségi jog egyéb rendelkezése ezt eleve nem zárja ki[19]. Ennek megfelelően néhány tagállam, mint például Olaszország, Ausztria vagy Luxemburg kiterjesztette az irányelvnek megfelelően elfogadott egyes nemzeti jogi rendelkezéseinek (mint például a biztonsági intézkedésekre vonatkozó rendelkezések) alkalmazását a jogi személyekre vonatkozó adatok feldolgozására is.

Az elhunyt emberekre vonatkozó információk tekintetében az adatkezelő gyakorlati intézkedései szintén jogi személyre vonatkozó olyan adatot eredményezhetnek, amely ténylegesen az adatvédelmi szabályok hatálya alá tartozik. Amikor az adatkezelő természetes és jogi személyekről különbségtétel nélkül gyűjt adatokat, és ugyanazon adatkészletbe foglalja őket, az adatfeldolgozás mechanizmusait és az ellenőrző

---

[18] Az irányelv (24) preambulumbekezdése: „mivel az adatfeldolgozással kapcsolatban a jogi személyek védelmére vonatkozó szabályokat ez az irányelv nem érinti”.

[19] Az Európai Bíróságnak a C-101/2001. sz. Lindqvist-ügyben 2003. november 6-án hozott ítéletének 98. pontja.

rendszert ki tudja úgy alakítani, hogy megfeleljenek az adatvédelmi szabályoknak. Valójában könnyebb az adatkezelő számára az adatvédelmi szabályokat az adatállományban található valamennyi információtípusra alkalmazni, mint megpróbálni kiválogatni, mi is vonatkozik természetes, és mi jogi személyekre.

IV. MI TÖRTÉNIK, HA AZ ADAT KÍVÜL ESIK A FOGALOMMEGHATÁROZÁSON?

Ahogyan e dokumentumban mindvégig láttuk, az adott információt bizonyos különféle körülmények között nem lehet személyes adatnak tekinteni. Ez fordul elő, amikor az adatot nem lehet egyénre vonatkozónak tekinteni, vagy mert az egyént nem lehet azonosítottnak vagy azonosíthatónak tekinteni. Amikor a feldolgozott információ nem tartozik a „személyes adat" fogalmába, annak az a következménye, hogy az irányelvet annak 3. cikke miatt nem lehet alkalmazni. Ez ugyanakkor nem jelenti azt, hogy egyéneket bizonyos helyzetekben mindenféle védelemtől meg lehet fosztani. A következő megfontolásokat kell figyelembe vennünk.

Attól, hogy az irányelvet nem lehet alkalmazni, a nemzeti adatvédelmi jogszabályokat esetleg még lehet. Amint a 34. cikk kimondja, az irányelv címzettjei a tagállamok. Az irányelv hatályán túl a tagállamokra nem vonatkoznak az általa előírt kötelezettségek, amelyek alapvetően azon törvényi, rendeleti és közigazgatási rendelkezések hatálybaléptetésére vonatkoznak, amelyek az irányelvnek való megfeleléshez szükségesek. Mindazonáltal az Európai Bíróság egyértelművé tette, hogy semmi sem akadályozza meg a tagállamokat abban, hogy az irányelv rendelkezéseit végrehajtó nemzeti jogszabályok hatályát kiterjesszék olyan területekre is, amelyek nem tartoznak az irányelv hatálya alá, hacsak a közösségi jog egyéb rendelkezése ezt eleve ki nem zárja. Ennélfogva könnyen megtörténhet, hogy egyes olyan helyzetek, amelyek nem érintik személyes adatoknak az irányelvben meghatározottak szerinti feldolgozását, ezek ellenére mégis a nemzeti jog védőintézkedései alá tartoznak. Ez alkalmazandó lehet például kulccsal kódolt adatokra, tekintet nélkül arra, hogy személyes adatok-e vagy sem.

Ahol az adatvédelmi szabályok nem alkalmazandók, bizonyos tevékenységek esetleg még mindig sérthetik az emberi jogokról szóló európai egyezmény 8. cikkét, amely védi a magán- és családi életet, figyelembe véve az EJEB messzire kiható ítélkezési gyakorlatát. Egyéb jogszabályrendszerek, mint például a kártérítési jog, a büntetőjog vagy a diszkriminációellenes jogszabályok szintén védelmet nyújthatnak az egyéneknek olyan esetekben, ahol az adatvédelmi szabályok nem alkalmazandók, és különféle jogos érdekek foroghatnak kockán.

V. KÖVETKEZTETÉSEK

E véleményében a munkacsoport iránymutatást nyújt annak módjáról, ahogyan a személyes adatnak a 95/46/EK irányelvben és a vonatkozó közösségi jogszabályokban található fogalmát értelmezni, és a különféle helyzetekben alkalmazni kell.

Általános megfontolásként került megjegyzésre, hogy az európai jogalkotó szándéka a személyes adat tág fogalmának elfogadása volt, bár e fogalom nem határtalan. Mindig szem előtt kell tartani, hogy az irányelvben található szabályok célja a személyes adatok feldolgozása terén az egyének alapvető jogainak és szabadságainak védelme, különös tekintettel a magánélet sérthetetlenségéhez való jogukra. E szabályokat tehát az olyan helyzetekre való alkalmazás érdekében alakították ki, amikor az egyének jogai

veszélyben lehetnek, és emiatt védelmet igényelnek. Az adatvédelmi szabályok hatályát nem szabad túlfeszíteni, de a személyes adat fogalmának indokolatlan korlátozását is kerülni kell. Az irányelv meghatározza saját hatályát, amely alól kizár számos tevékenységet, és rugalmasan kezeli a szabályok alkalmazását a hatálya alá tartozó tevékenységek tekintetében. Az adatvédelmi hatóságok elengedhetetlen szerepet játszanak az ezen alkalmazás terén kívánatos megfelelő egyensúly kialakításában (lásd a II. bekezdést).

A munkacsoport elemzése a „személyes adat" meghatározásában elkülöníthető négy fő „alkotóelemre" épül, úm. „bármely információ", „vonatkozó", „azonosított vagy azonosítható", „természetes személy". Ezek az elemek szorosan egybefonódnak, és kölcsönösen erősítik egymást, de együttesen határozzák meg, hogy az adott információt „személyes adatnak" kell-e tekinteni. Az elemzést az európai adatvédelmi hatóságok nemzeti gyakorlatából vett példák támasztják alá.

- Az első elem – „bármely információ" – a fogalom tág értelmezését igényli, tekintet nélkül az információ természetére vagy tartalmára, valamint azon technikai formátumra, amelyben megjelenítették. Ez azt jelenti, hogy a személyre vonatkozó objektív és szubjektív információt – forduljon elő bármely rendeltetésében – egyaránt „személyes adatnak" lehet tekinteni, függetlenül a műszaki hordozótól, amelyen tárolják. A vélemény továbbá tárgyalja a biometrikus adatokat és jogi megkülönböztetésüket azon emberi mintáktól, amelyekből kinyerték őket (lásd a III. bekezdés 1. pontját).

- A második elemet – „vonatkozó" – ez idáig gyakran figyelmen kívül hagyták, noha elengedhetetlen szerepet játszik a fogalom alanyi hatályának meghatározásában, különösen a tárgyakkal és új technológiákkal való kapcsolatokban. A vélemény három alternatív elemet hoz fel – úm. tartalom, cél és eredmény – annak meghatározására, hogy az információ egyénre „vonatkozó"-e. Ez lefed továbbá olyan információt is, amelynek egyértelmű hatása lehet arra, amilyen bánásmódban az egyént részesítik vagy ahogyan értékelik (lásd a III. bekezdés 2. pontját).

- A harmadik elem – „azonosított vagy azonosítható" – azokra a feltételekre összpontosít, amelyek mellett az egyént „azonosíthatónak" kell tekinteni, és különösen azokra a „módszerekre" irányul, amelyeket az adatkezelő vagy más személy valószínűleg felhasználna az említett személy azonosítására. Az adott eset sajátos összefüggései és körülményei fontos szerepet játszanak ezen elemzésben. A vélemény foglalkozik továbbá a „pszeudonimizált adatokkal" és a „kulccsal kódolt adatok" használatával a statisztikai és gyógyszeripari kutatások terén (lásd a III. bekezdés 3. pontját).

- A negyedik elem – „természetes személy" – annak követelményével foglalkozik, hogy a „személyes adatoknak" „élő egyénekre" kell vonatkozniuk. A vélemény tárgyalja továbbá az elhunyt személyekre, a még meg nem született gyermekekre és a jogi személyekre vonatkozó adatokkal meglévő közös határfelületet is (lásd a III. bekezdés 4. pontját).

A vélemény végezetül elemzi, mi is történik, ha az adat a „személyes adat" fogalommeghatározásának hatályán kívül esik. Eltérő megoldások adódhatnak az ilyen esetekben felmerülő problémák megoldására, ideértve az irányelv hatályán kívül eső nemzeti jogot, amennyiben az egyéb közösségi jogszabályokat tiszteletben tartják (lásd a IV. bekezdést).

A munkacsoport felkér valamennyi érdekelt felet, hogy alaposan tanulmányozza az e véleményben kifejtett iránymutatást, és vegye figyelembe, amikor a nemzeti jog rendelkezéseit értelmezi és alkalmazza a 95/46/EK irányelvvel összhangban .

A munkacsoport tagjai, főképpen a nemzeti szintű adatvédelmi felügyelő hatóságok képviselői elkötelezték magukat az e véleményben kifejtett iránymutatásnak a hatáskörük alá tartozó továbbfejlesztése mellett, valamint nemzeti joguk megfelelő alkalmazásának biztosítása mellett a 95/46/EK irányelvvel összhangban.

A munkacsoport szándéka az e véleményben kifejtett iránymutatást alkalmazni és továbbfejleszteni, ahol ez helyénvaló, valamint gondosan figyelembe venni későbbi munkájában, különösen amikor olyan témákkal foglalkozik, mint például a személyazonosság kezelése az e-kormányzat és az e-egészségügy, továbbá az RFID területén. Ami ez utóbbit illeti, a munkacsoport hozzá kíván járulni egy olyan további elemzéshez, amely annak módjára összpontosít, ahogyan az adatvédelmi szabályok hatást gyakorolhatnak az RFID-k használatára, témája továbbá olyan kiegészítő intézkedések esetleges meghozása, amelyekre alkalmasint azért lehet szükség, hogy az adatvédelmi jogokat és érdekeket az említett kontextusban megfelelően tiszteletben tartsák.

A munkacsoport végezetül szívesen lát minden visszajelzést az érdekelt felek és az felügyelő hatóságok részéről az e véleményben található iránymutatással kapcsolatos gyakorlati tapasztalataikról, valamint bármely további példát a dokumentumban említetteken túl. A munkacsoport kellő időben vissza kíván térni a témához, tekintettel a személyes adat alapfogalma közös értelmezésének továbbfejlesztésére, valamint a 95/46/EK irányelv és az irányelv alapján kapcsolódó közösségi joganyag harmonizált alkalmazása és helyesebb végrehajtása érdekében.

---

a munkacsoport részéről

az elnök
Peter SCHAAR