Írta:
ALEXIN ZOLTÁN

A SZEMÉLYES ADATOK VÉDELMÉNEK JOGI, ETIKAI ÉS INFORMATIKAI KÉRDÉSEI

Egyetemi tananyag

TYPOTEX

2011

LEKTORÁLTA: Dr. Könyves-Tóth Pál, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar

TÁMOGATÁS:
Készült a TÁMOP-4.1.2-08/1/A-2009-0008 számú, „Tananyagfejlesztés mérnök informatikus, programtervező informatikus és gazdaságinformatikus képzésekhez” című projekt keretében.

ISBN 978-963-279-489-1

KÉSZÜLT: a Typotex Kiadó gondozásában
FELELŐS VEZETŐ: Votisky Zsuzsa
AZ ELEKTRONIKUS KIADÁST ELŐKÉSZÍTETTE: Erő Zsuzsa

KULCSSZAVAK:
személyes adatok védelme, információs önrendelkezés, adatvédelmi jog, alapvető emberi jogok, Európai Unió adatvédelmi rendszere, adatkezelés etikája, tisztességes adatkezelés, fizikai védelem.

ÖSSZEFOGLALÁS:
A XXI. században diplomát szerző informatikus hallgatók képzéséből nem hiányozhatnak a személyes adatok kezelésével kapcsolatos alapvető ismeretek. A jegyzet a képzéshez szükséges ismereteket rendszerezett formában tartalmazza. A tizenhárom fejezet figyelembe veszi az egyetemi képzés szemesztereinek hosszát. Alkalmas előadás, illetve előadás és szemináriumi formában történő oktatásra, valamint távoktatásra is. Tárgyalja a megértéshez szükséges minimális jogi ismereteket, illetve a személyes adatok védelméhez való jognak az emberi méltóság alapjogából levezethető gyökereit. Feldolgozza a fontosabb nemzetközi egyezményeket és az Európai Unió adatvédelmi dokumentumait, ismerteti a fontosabb magyar adatvédelmi jogi megoldásokat és jogszabályokat.

A jegyzetben olyan etikai kérdések is megvitatásra kerülnek, amelyek kapcsolódnak a magán- és családi élet tiszteletben tartásához, a tisztességes adatkezelés alapelvéhez.

A jegyzet néhány kiemelkedő személyiség rövid életútját és munkásságát is ismerteti

TARTALOM

1. Bevezetés és történeti áttekintés

Ez az egyetemi jegyzet informatikus szakos hallgatók számára készült, amelyet a szerző a Szegedi Tudományegyetem Informatikai Tanszékcsoportjában a hasonló című előadásához készített. A jegyzet célkitűzése az, hogy a természettudományos műveltséggel rendelkező hallgatókat megismertesse a személyes adatok védelmének humán aspektusaival, emberi jogi kérdéseivel, és a témához kapcsolódó morális, etikai és jogi irodalomból ismereteket közvetítsen a számukra.

Informatikai szempontból az adatvédelem titkos jelszavakat, beléptető rendszereket, betonbunkereket jelent, azaz az adatok fizikai védelmét. Ha azonban a kérdést emberi jogi oldalról vizsgáljuk, a fizikai adatvédelem a probléma egy kis szeletét jelenti csupán. A fizikai védelemnél sokkal komolyabb társadalmi kérdésekről esik szó, például az önrendelkezésről, az emberi méltóságról, a szabadságról, a megfigyelésről, és a személyes adatok felhasználásának kérdéseiről. Ezek az emberi jogi szempontok jelenleg nem jelennek meg a szoftvertervezők szempontrendszerében, az informatikai infrastruktúra üzemeltetésekor, de még a magyar jogalkotásban sem. Ezért nagy szükség van arra, hogy a személyes adatok védelmének kérdései az egyetemi oktatásban is szerepeljenek.

A személyes adatok védelme nagyon fiatal alapvető emberi jog. Nem tekint vissza olyan nagy múltra, mint például a lakóhely megválasztásának joga, a szólás- vagy a vallásszabadság. Utóbbiak már több száz éve jelen vannak a társadalomtudományokban, és mintegy kétszáz éve a fejlett államok alkotmányaiban[1] és ennyi idő alatt jelentős mennyiségű tapasztalat halmozódott fel a jog értelmezésében, alkalmazásában és a peres ügyekben. Az adatvédelemről ez nem mondható el. Jelenleg az Európai Unió szintjén sincs stabil és kiforrott értelmezése az adatvédelemhez fűződő alapjog kiterjedésének, definíciójának. A bíróságok ítélkezési gyakorlata az első tétova lépéseket mutatja. Ezt felismerve az Európai Unió emberi jogi szervei, elsősorban az Európai Bizottság kiemelten foglalkozik a személyes adatok védelmének jogával, a kérdést napirenden tartja, és küszöbön áll a szabályozás nagyobb mértékű átalakítása.[2]

Az Európai Unió tagállamaiban élők számára az adatvédelemhez való alapvető jog tulajdonképpen 2009. december 1-je óta létezik. Attól a dátumtól fogva, hogy a 25 tagállam mindegyike ratifikálta az Európai Unió reformegyezményét, a Lisszaboni Egyezményt, amely beemelte és minden tagállam számára kötelezővé tette az Alapvető jogok chartáját (az Egyesült Királyság és Lengyelország kapott bizonyos engedményeket). Ebben konkrétan leírva szerepel a személyes adatok védelméhez való jog. Korábban ez a szókapcsolat nem szerepelt a nemzetközi dokumentumokban, helyette a magán- és családi élethez való jog, a magánlakás, a kommunikáció háborítatlansága, a lakóhely szabad megválasztása, a magánélethez való jog stb. szerepelt, amely csak implicit módon foglalta magába a személyes adatok védelméhez való jog egy részét.

Az informatika megjelenése előtt, a személyes információk védelmét a magánélethez való jog foglalta magába. A magánélet (privacy) védelme, a magánélet háborítatlanságához fűződő jog, nem terjed ki *minden* személyes adat védelmére, csak bizonyos adatokéra. Az

[1] Például az Emberi és polgári jogok nyilatkozata, 1789., (*La Déclaration des droits de l'Homme et du citoyen*), vagy az Egyesült Államok alkotmánya, 1787. (*Bill of Rights*).

[2] Az Európai Bizottság közmeghallgatást tartott a személyes adatok védelméhez fűződő alapvető jog szabályozásának jövőjéről.

Emberi Jogok Európai Bírósága számos ítéletében foglalkozott a problémával és végül az ítéletekben kimondták, hogy pl. a személynevek, egyes eseményeken részt vett személyek névsora nem tartozik a magánélethez. Ezért az ilyen adatok kezelése, felhasználása és továbbítása nem sérti a magánélet háborítatlanságához fűződő jogot. Továbbá a védelemben részesített adatok esetén is csak bizonyos felhasználások sértik a magánszférát, míg más felhasználások nem. A személyes adatok védelme azonban már kiterjed minden személyes adatra és minden felhasználásra.

A személyes adatok védelme szoros kapcsolatban áll a közérdekű adatok nyilvánosságával, azaz hogy az állampolgárok hozzá tudjanak jutni a sorsukat befolyásoló adatokhoz. Az emberi méltósághoz a személyiség szabad kibontakoztatása is hozzá tartozik, ez pedig csak akkor képzelhető el, ha az egyén a társadalom hasznos és cselekvő tagja tud lenni, melynek fontos tényezője a közérdekű adatokhoz jutás. Magyarország mind a két jogot egy közös törvényben, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényben szabályozza. A nemzetközi irodalomban a magánélet védelme magában foglalja a közérdekű adatokhoz történő hozzájutás jogát. Néhány nevezetes ítélet is született már az európai bíróságokon: ezek szerint pl. a magánélet része a lakóhely szabad megválasztásának joga, és ez magában foglalja az adott földrajzi helyen rendelkezésre álló környezetvédelmi, szennyezési adatok nyilvánosságát is. A magánélet a döntési autonómiát is magában foglalja. Ezért az USA legfelsőbb bírósága, amely ott alkotmánybírósági feladatokat is betölt, erre hivatkozva nem tiltja meg az abortuszt (pedig ez gyakran felmerül). Az utódok létrehozásának időpontjára és módjára vonatkozó *döntésben* az egyének autonómiája elengedhetetlen.

Az elmúlt kétezer év történelmében a személyhez fűződő jogok fokozatos fejlődése figyelhető meg. Kezdetben a személyes biztonsághoz a testi épséghez való jog kapott hangsúlyt, majd kis idő múlva megjelent a dolgokhoz kapcsolódó, pl. ingó és ingatlan tulajdonhoz való jog, valamint a tulajdonnal való szabad rendelkezés joga. A későbbiekben a dolgokhoz kapcsolódó jog egyre inkább virtualizálódott és olyan elvi kérdések is fontossá váltak, mint a vallásszabadság, a gondolkodás szabadsága, és a szabad véleménynyilvánítás joga, a magánlakás biztonsága és sérthetetlensége, továbbá a kommunikáció és a társas kapcsolatok szabadsága, és legvégül érkezünk el a személyiség absztrakt lenyomatát jelentő személyes adatokhoz, az azokkal való rendelkezés szabadságához.

A magánlakás sérthetetlensége érdekében szenvedélyesen szólalt fel az angol parlamentben id. William Pitt parlamenti képviselő 1763-ban.[3] A történet a kanadai éves adatvédelmi konferencián hangzott el 2005-ben:

> A legszegényebb ember is keményen dacolhat házában a király minden erejével. Lehet az gyenge, a tető rozoga, a szél keresztülfújhat rajta, a vihar tépheti, az eső beeshet, de Anglia királya oda nem léphet be. Semmilyen erővel nem merészelheti átlépni e kis rom küszöbét.

A nem tárgyakhoz kötődő személyi, személyiségi jogokat a magyar jogelmélet (és az alkotmánybíróság is) az emberi méltósághoz (human dignity) való jogból vezeti le. Ez egy olyan fogalom, ami az ép tudattal rendelkező, mentálisan egészséges embernek van csupán

[3] *Kosseim, P.:* Health Information Privacy, (a kanadai adatvédelmi biztos munkatársának nyitó előadása), in *4th Annual Health Information Privacy Conference*, Jan 27. Toronto, Kanada, 2005.
The poorest man may in his cottage bid defiance to all the forces of the crown. It may be frail, its roof may shake, the wind may blow through it, the storm may enter, the rain may enter, but the King of England cannot enter! All his force dares not cross the threshold of the ruined tenement!

és a szellem szabadságát, az egyéni autonómiát, önrendelkezést, önmegvalósítást, önfejlődést, de a tisztességes halált is magába foglalja. Az adatvédelemhez fűződő jogot is az emberi méltóság *anyajogából* vezetik le.

Az évszázados jogi fejlődés során kikristályosodott az az alapelv, hogy mivel emberi méltósága is csak élő embernek lehet, így személyhez fűződő jogai is **élő** személynek lehetnek csupán. Ezt az alapelvet az adatvédelem alaposan felforgatja (majd), mert megjelenik a még meg nem született magzat (akár megtermékenyített petesejt) adataival való rendelkezés problémája, vagy ami még ennél is fontosabb: társadalmi szinten elfogadhatatlan az, hogy az elhaltak személyes adatainak jogi védelme a halál pillanatában megszűnjön. Ezt a morális és etikai problémát a jognak kezelni kell és ez be is fog következni.

1.1. A jegyzet használata

A jegyzetben számos esetben történik hivatkozás jogi dokumentumokra. Ezek jelentős része az Interneten megtalálható, hivatalos szerverekről letölthető.

Az Európa Tanács nemzetközi egyezményeinek szövege és adatai a Council of Europe – Treaty Office hivatalos weboldaláról tölthetők le (http://conventions.coe.int/). Ezen az oldalon találhatjuk meg az egyezmények hivatalos (angol és francia) szövegét, a hozzá fűzött magyarázatokat, az aláíró országokat, és az aláírások, törvénybe iktatások, hatályba lépések, valamint derogációk időpontját az egyes országokban, így Magyarországgal kapcsolatban is.

A strasbourgi Emberi Jogok Európai Bírósága (http://www.echr.coe.int) honlapján a bíróság működésének részletes bemutatását, az indítványok benyújtásának módját, dokumentumokat, a bíróság eddigi ítéleteit lehet tanulmányozni, keresni. A luxemburgi székhelyű Európai Unió Bírósága (http://curia.europa.eu) honlapján információkat találhatunk a bíróság működéséről, és kereshetünk a régi ügyek között.

A Magyar Köztársaság Alkotmánybíróságának honlapján (http://www.mkab.hu) találhatjuk meg az Alkotmány hivatalos, magyar és angol nyelvű szövegét, valamint az Alkotmánybíróságról szóló 1989. évi XXXII. törvény hatályos szövegét, az Alkotmánybíróság korábbi összes határozatát, és a még el nem bírált indítványok összefoglaló adatait.

A Parlament által alkotott új törvényeket, a Kormány és a minisztériumok által kibocsátott rendeleteket a Magyar Közlöny (http://www.kozlonyok.hu) weboldalán találhatjuk meg. A Magyar Közlöny a Magyar Köztársaság hivatalos lapja. Ez tartalmazza az összes újonnan megjelent jogszabályt. Ezekből egyes államigazgatási területek számára tematikus válogatás is készül pl. Egészségügyi Közlöny, Egészségbiztosítási Közlöny, Honvédelmi Közlöny, Igazságügyi Közlöny stb. amely ennek a területnek az új jogszabályait tartalmazza. Ezek a tematikus közlönyök a Magyar Közlönyben megjelent jogszabályokból az adott területre vonatkozókat tartalmazzák csak, és helyet adnak az adott minisztérium egyéb közleményeinek is (pl. álláshirdetések, pályázatok, felhívások, miniszteri utasítások). A tematikus közlönyök is ingyenesen megtekinthetők a weboldalon. Ezen az oldalon találhatjuk meg az Alkotmánybíróság Határozatait tartalmazó folyóiratot is, amely kéthavonta jelenik meg. A jogalkotásról szóló 1987. évi XI. törvény 14. §-a szerint minden jogszabályt a Magyar Köztársaság hivatalos lapjában, a Magyar Közlönyben ki kell hirdetni. Az elektronikus információszabadságról szóló 2005. évi XC. törvény harmadik fejezete gondoskodik arról, hogy az előkészítés alatt álló jogszabálytervezetek, a Parlamentnek benyújtott javas-

latok és módosító indítványok továbbá, hogy a Magyar Közlöny az Interneten, nyilvános honlapon megjelenjenek. A Magyar Közlönyből évente 150-200 szám jelenik meg, amelyek összesen mintegy százezer oldalnyi új jogszabályt tartalmaznak.

A magyar Parlament (http://www.parlament.hu) honlapján a törvényalkotás folyamatát lehet követni, a törvényjavaslat eredeti szövegét, a módosításokat, a bizottsági munkát, a szavazások eredményt és a köztársasági elnöknek elküldött végleges törvényszöveget, majd pedig a törvényt kihirdető Magyar Közlöny adatait (évfolyam, szám) tekinthetjük meg.

Az eMagyarország Kormányzati Portálon (http://www.magyarorszag.hu) a Keresés/Jogszabály-kereső szolgáltatás alatt a Magyarországon hatályos összes jogszabály (törvény, Kormányrendelet vagy miniszteri rendelet) szövege megtalálható, kereshető és másolható. A hivatkozott jogszabály megjelenési évét, számát és a jogalkotót (Kormány, valamilyen minisztérium) kiválasztva kereshetünk az adatbázisban.

A magyar bíróságok fontosabb ítéleteinek anonimizált szövege elérhető a (http://www.birosag.hu) weboldalról a Bírósági Határozatok Gyűjteményében. Alapvetően a polgári perek jogerős ítéleteiről van szó, illetve a Legfelsőbb Bíróság Jogegységi Határozatairól.

Az országgyűlési biztosok honlapjai a (http://www.obh.hu) az általános ombudsmani hivatal nyitólapjáról érhetők el a legkönnyebben. Az adatvédelmi biztos feliratra kattintva juthatunk el az Adatvédelmi Biztos Hivatalának honlapjához. Az adatvédelmi biztos honlapját közvetlenül is elérhetjük a http://www.adatvedelmibiztos.hu címen. Itt megtaláljuk a biztos közleményeit, néhány törvény szövegét, a biztos közleményeit és állásfoglalásait, a hivatalra vonatkozó közérdekű adatokat.

1.2. Néhány alapvető jogi ismeret

A Magyarországon érvényes jogszabályokat egyelőre a jogalkotásról szóló 1987. évi XI. törvény alapján készítik el. Az Alkotmánybíróság nemrégen a teljes törvényt alkotmányellenesnek nyilvánította, és a törvényt megsemmisítette *pro futuro* 2010. december 31-i határidővel. Az odáig terjedő időszakban a Parlamentnek új jogalkotási törvényt kell elfogadnia.[4] Ez a javaslat elkészült és már a Parlament előtt van.[5]

A jogalkotásról szóló törvény szerint a jogszabályokat szabványos módon kell elnevezni, amely tartalmazza a jogszabály címét, éven belüli sorszámát, kibocsátás évét, rendeletnél a kibocsátás napját és a kibocsátót, és végül a jogszabály típusát. Például: *az Alkotmánybíróságról szóló 1989. évi XXXII. törvény*, vagy *az emberen végzett orvostudományi kutatások végzéséről szóló 23/2002. (V. 9.) EüM rendelet*.

A Magyar Köztársaságban a jogszabályok hierarchiája a következő:

Alkotmány – törvény – Kormányrendelet – különböző rendeletek.

A legfontosabb jogszabály a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény. Formailag törvény, de annál jelentősebb a szerepe. Ez képezi az összes további jogszabály alapját. Benne találhatók például az államhatalom formájára, megszervezésére, az alapvető jogokra és kötelezettségekre, a Parlament, a köztársasági elnök és a Kormány

[4] Az új törvényt a Jogalkotásról szóló 2010. évi CXXX. Törvény, amely 2011. január 1-jétől hatályos.
[5] A 121/2009. (XII. 17.) számú AB határozat megjelent a Magyar Közlöny 2009. évi 184. számában.

működésére vonatkozó paragrafusok. Az Alkotmányon a rendszerváltáskor jelentős mértékű változtatásokat hajtottak végre, azonban továbbra is ideiglenes maradt. A 2010-ben hatalomra került FIDESZ Kormány egy teljesen új Alkotmány elkészítését ígéri. A hatályos Alkotmány szerint háromféle jogszabály létezik: a Parlament által elfogadott törvény, a törvények végrehajtását elősegítő, a Kormány által kiadott Kormányrendelet[6], illetve a Kormány tagjai, azaz a miniszterek által kibocsátott miniszteri rendelet.[7]

Az Alkotmány 35. § (2) bekezdése szerint:

> (2) A Kormány a maga feladatkörében rendeleteket bocsát ki, és határozatokat hoz. Ezeket a miniszterelnök írja alá. A Kormány rendelete és határozata törvénnyel nem lehet ellentétes. A Kormány rendeleteit a hivatalos lapban ki kell hirdetni.

Az Alkotmány 37. § (3) bekezdése szerint:

> (3) A Kormány tagjai törvényben vagy kormányrendeletben kapott felhatalmazás alapján feladatkörükben eljárva rendeletet adnak ki, amelyek törvénnyel és kormányrendelettel nem lehetnek ellentétesek. A rendeleteket a hivatalos lapban ki kell hirdetni.

Amennyiben bármely személy úgy találja, hogy egy miniszteri rendelet (vagy egy részlete) ellentétes lenne egy törvénnyel vagy egy Kormányrendelettel, illetve egy Kormányrendelet (vagy egy bizonyos részlete) ellentétes lenne egy törvénnyel, akkor az Alkotmánybírósághoz fordulhat[8], és indítványában kérheti a jogszabály utólagos felülvizsgálatát. Az indítványban meg kell jelölnie ezt a törvényt (amellyel ellentétes a megsemmisíteni kívánt jogszabályrészlet) és indokolni kell, hogy miért ellentétes ezzel a Kormányrendelet vagy a miniszteri rendelet. Ha az indoklással az Alkotmánybíróság egyetért, akkor a kért jogszabályrészletet megsemmisíti. Az indoklás nélküli indítványokat az AB hivatalból elutasítja. Általában teljes jogszabályt nem szoktak megsemmisíteni, hanem annak csak bizonyos részét.

A jogalkotásról szóló 1987. évi XI. törvény és az Alkotmány a fentebb felsoroltakon kívül másféle jogszabályt nem ismer. Azonban vannak még olyan, a rendszerváltás előtt keletkezett jogszabályok pl. elnöki tanácsi rendeletek, amelyek érvényben maradtak a rendszerváltás után is. A közelmúltban egynek a törlését kérte egy indítványozó az Alkotmánybíróságtól azon az alapon, hogy az ellentétben áll a jogalkotási törvénnyel. Az AB azonban elutasította az indítványt, mert a hivatkozott elnöki tanácsi rendeletet nem találta alkotmányellenesnek. A legrégebbi hatályban lévő törvény az 1827. évi XII. törvény arról, hogy kik voltak azok a neves személyiségek, akik az MTA alapításában nagy szerepet játszottak.[9]

A jogszabályokra történő hivatkozás során általában nem elegendő pl. egy törvény megnevezése, hanem szükséges azon belül pontosabb megjelölés is. A jogszabályok para-

---

[6] Az Alkotmány, Parlament, Kormány, és a Kormányrendelet szavak az MTA Nyelvtudományi Intézet által kiadott Helyesírási Szabályzat szerint nagybetűvel írandók.

[7] Az alkotmány 7/A. § (2) bekezdése szerint:
(2) Jogszabály a törvény, a kormányrendelet, a Magyar Nemzeti Bank elnökének rendelete, a miniszterelnöki rendelet, a miniszteri rendelet, a Pénzügyi Szervezetek Állami Felügyelete elnökének rendelete, a Nemzeti Média- és Hírközlési Hatóság elnökének rendelete és az önkormányzati rendelet. Jogszabály továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kibocsátott rendelete.

[8] Az Alkotmánybíróságról szóló 1989. évi XXXII. törvény szerint még számos más okból is az Alkotmánybírósághoz lehet fordulni, jogszabály egy-egy rendelkezésének megsemmisítése céljából.

[9] 1827. évi XII. törvény szócikk a Wikipédián

grafusokból (szakaszokból) állnak, amelyeket egyesével növekvő sorszámozással látnak el és utánuk a § jelet írják.[10] A paragrafusokban bekezdések találhatók, illetve felsorolások. A bekezdéseket szükség szerint (1), (2), … számokkal azonosítják; a felsorolásokat a), b), c) … betűkkel[11], vagy 1., 2., 3., … sorszámokkal jelölik. A fentiek szerint egy pontos *jogszabályi hely* megadása lehet a következő: A jogalkotásról szóló 1987. évi XI. törvény 1. § (1) bekezdésének b) pontja.

A jogszabályokat a hierarchiában vele azonos szinten álló másik jogszabállyal lehet módosítani. Törvényt egy másik törvénnyel, Kormányrendeletet egy másik Kormányrendelettel stb. A módosításról szóló jogszabályt olyan módon hajtják végre, hogy a hatályba lépése napján a benne leírt utasítás szerint módosítják a korábbi szöveget. Lehet új paragrafust beszúrni, paragrafust törölni, bekezdést beszúrni, törölni, paragrafus vagy bekezdés szövegét újabbra cserélni, gyakorlatilag teljesen szabadon. A módosító jogszabály ezután hatályát is veszti – ezzel szabad utat enged a további módosításoknak. A régi jogszabály pedig a megváltozott tartalommal lesz érvényes. Mivel főként az alacsonyabb rendű jogszabályok gyakran változnak, ezért az **Interneten megtalált jogszabály szövegek használata veszélyes**, mert gyakran nem tartalmazzák a legfrissebb módosításokat. Ezért, ha valaki ezekre alapoz egy pert, jogi cselekményt, akkor könnyen elszámíthatja magát. Minden esetben a legújabb, hiteles, az összes módosítás átvezetését tartalmazó jogszabályt kell használni, amit legegyszerűbben az eMagyarország Kormányzati portálon találhatunk meg. Egyes jogi informatikai szolgáltató cégek, havi előfizetési díj ellenében folyamatosan karbantartott jogszabály adatbázishoz engednek hozzáférést. Nagyobb vállalkozásoknál az előfizetés a budapesti Complex Kft. (http://www.complex.hu) vagy az Opten Kft. (http://www.opten.hu) stb. szolgáltatásaira létszükséglet.

A módosított jogszabályok az eredeti címmel és számmal érhetők el az adatbázisokban – ez biztosítja azt, hogy azokat a jól ismert nevük alapján továbbra is meg lehessen találni. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt már sokszor módosították[12], ennek ellenére a fokozatosan változó szöveg minden esetben az 1992-es eredeti törvényre hivatkozással érhető el.

A törvények és rendeletek megnevezése és címe általában hosszú, ezért sok, gyakran használt jogszabálynak van meghonosodott rövidítése. Ezek használata jogi szövegekben elkerülhetetlen, mert egyébként a dokumentum nagy része csak a jogszabályok szabvány neveit sorolná állandóan. A jogalkotásról szóló 1987. évi XI. törvény rövidítése a Jat., a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rövidítése: Avtv., az egészségügyi és a hozzájuk tartozó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény rövidítése: Eüaktv., az egészségügyről szóló 1997. évi CLIV. törvény rövidítése Eütv., és még számos ilyen van. A jegyzet további fejezeteiben ezeket a rövidítéseket gyakran fogjuk használni.

A magyar bíróságokon az eljáró bírók ítélkezésük során egyedül a törvényeket kell, hogy figyelembe vegyék. Mivel Magyarországon a joganyag gyorsan változik, ezért a jogszabályok értelmezése nem tud stabilizálódni, így egy hektikus ítélkezési gyakorlat alakult

[10] Ha több paragrafust szúrnak be utólag egy jogszabályba, akkor előfordul a 6/A. §, 6/B. § jelölés is azért, hogy ne kelljen teljesen átsorszámozni egy meglévő törvény paragrafusait.
[11] Bonyolult felsorolások esetén előfordul kétszintű hierarchia és akkor a címkék: a) aa), ab), ac), b), ba), bb), c), …, illetve ha a felsorolás elérte a z) címkét, akkor is megjelenhet a címkék között a … z), aa), ab), ac), … címke.
[12] Könyves-Tóth Pál: Az adatvédelmi törvény metamorfózisai, Fundamentum emberi jogi folyóirat 2/2010. szám.

ki. Az egyes bíróságok ugyanolyan esetekben ellenkező módon értékelik a jogi helyzetet. Tömegesen jelentkező ügyekben bírói konferenciákon keresik a legjobb gyakorlatot, illetve a Legfelsőbb Bíróság jogegységi határozatokat adhat ki, azonban az egészet romba döntheti az, ha a Parlament közben megváltoztatja a törvényt. Az Eüaktv. pl. tizenhárom év alatt mintegy harmincszor változott meg.

Egyedi, alapvetően fontos ügyekben egyre jelentősebb szerepet kap az ún. esetjog (case law), ami azt jelenti, hogy ítélethozatalkor a bíróság áttekinti a hasonló témában hozott ítéleteket és indoklásaikat. Amennyiben van precedens, azaz hasonló ügy és abban született ítélet, akkor egyszerűen azt alkalmazzák. A magasabb bíróságok, pl. Emberi Jogok Európai Bírósága, vagy az Alkotmánybíróság szinte kivétel nélkül precedensbíróságok. Ez összefügg e bíróságok tekintélyével és egyedülálló szerepével. A bíróságok tekintélyének sokat ártana, ha eltérően ítélnének meg hasonló ügyeket, másrészt a nagy jelentőségű ügyekben nem igazán akad olyan másik bíróság, amely ugyancsak eljárna. Az esetjog a felkészült jogászoknak sokat segít, és jól megjósolhatóvá teszi az ügyek kimenetelét. Ezért van egy olyan tendencia, amely szerint a bíróságok a nehezebb ügyekben egyre inkább precedensbíróságokká válnak.

1.3. Napjaink időszerű adatvédelmi kérdései

A médiában gyakran találkozunk aktuális adatvédelmi problémákkal. Az adatvédelmi jogszabályok mechanikus alkalmazása azonban rendszerint nem vezet el a helyes és tisztességes megoldáshoz. Az államhatalom Magyarországon hetek alatt alkothat törvény valamilyen személyes adat megszerzésére, ugyanakkor ez jelentősen sértheti az állampolgárok alapvető jogait, emberi méltóságát. Az állampolgári jogok biztosa, az adatvédelmi biztos, valamint civil szervezetek is egyre gyakrabban alkotnak véleményt egy-egy tervezett jogszabályról, annak hatásairól, következményeiről. Némely esetben már sikerült egy-egy kérdést megegyezéssel, megnyugtató módon kezelni.

A belpolitikában jelenleg napirenden tartott témák: banki adósok országos nyilvántartásának kérdése; távközlési szolgáltatók adatmegőrzési kötelezettsége; megfigyelő kamerák telepítése közterületen, közlekedési eszközökön; munkavállalók adatvédelemhez fűződő jogainak kérdése; a szocializmus állambiztonsági nyilvántartásában őrzött adatok kezelése; a (nemzetközi) pénzügyi tranzakciók biztonsága; a társadalombiztosítás országos adatgyűjtése; országgyűlési választásokkal kapcsolatban gyűjtött személyes adatok problémája; iskolai tanulók, egyetemi hallgatók személyes adatainak kezelése; közösségi oldalakkal kapcsolatos adatvédelem.

Az adatvédelemben megnyugtató módon eddig nem megoldott kérdések a következők: családi személyes adat; a különleges személyes adat definíciója; halottak személyes adatainak védelme; anonimizálás, pszeudonimizálás, és kódolás; hosszú időre szóló személyes egészségügyi adatok kezelésének alapelvei; PIA (privacy impact analysis); személyes adatok megbízható törlése; biometrikus azonosítás; genetikai adatbázisok személyes adatainak védelme.

Ellenőrző kérdések

1. Milyen előzményei vannak a személyes adatok védelméhez fűződő alapvető jognak?

2. Miért nevezik személyhez fűződő jognak a személyes adatok védelméhez való jogot?

3. Milyen jogszabálytípusok fordulnak elő Magyarországon?

4. Mi a jogszabályok hierarchiája?

5. Mely törvény szabályozza a jogszabályok létrehozását?

6. Az állampolgárok tudomást szerezhetnek-e a rájuk vonatkozó, hatályos jogszabályokról?

7. Hogyan lehet egy létező jogszabályt módosítani?

8. Hogyan nevezik el a jogszabályokat?

9. Mi a precedensjog vagy esetjog?

10. Mikor lehet az Alkotmánybírósághoz fordulni?

11. Mi a jogszabályi hely?

12. Soroljon fel néhány aktuális magyar adatvédelmi társadalmi problémát!

2. Alapvető fogalmak és meghatározások

Az alábbi alapfogalmak a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 2. §-ában találhatók. Jogi, peres ügyekben mindenképpen ezek képezik az eljárások alapját. Természetesen ezek a fogalmak a hétköznapi életben, a munkahelyeken, a tudományos életben is magyarázhatók és pontosabbá tehetők.

További igen részletes elemzés található ezekről a fogalmakról Dr. Jóri András: Adatvédelmi Kézikönyvében. Ugyanakkor a bíróságoknak alapvetően a törvények szövegéből kell kiindulniuk és nem kötelesek más véleményt figyelembe venni.

1. személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

2. különleges adat:

a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra,

b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat;

3. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

4. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől;

5. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

6. hozzájárulás: az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez;

7. tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

8. adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;

9. adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is;

10. adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik;

11. nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

12. adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

13. adatzárolás: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;

14. adatmegsemmisítés: az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;

15. adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;

16. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából – beleértve a jogszabály rendelkezése alapján történő megbízást is – személyes adatok feldolgozását végzi;

Figyeljük meg, hogy a személyhez kapcsolható adatokon belül egy érzékenyebb adatcsoportot különített el a törvény: az ún. *különleges* személyes adatok körét. Elvileg a különleges személyes adatok fokozottabb védelmet élveznek más – közönséges – személyes adatokkal összehasonlítva. A különleges személyes adatok között találjuk a bűnügyi személyes adatokat, a személyes egészségügyi adatokat, a világnézetre, vallásra vonatkozó személyes adatokat. Ezek kinek-kinek a legbizalmasabb magánügyei közé tartoznak. Magától értetődően a szexuális életre vonatkozó személyes adatok is ide kerültek.

Az Európai Unió országaiban a különleges személyes adatok kezelése általában tilos. Ez alól néhány kivétel van: különleges személyes egészségügyi adatokat lehet kezelni, ha arra a megelőzés, a diagnosztika és a terápia céljából vagy egészségügyi intézmények irányítása érdekében szükség van, illetve bűnügyi és más különleges személyes adatokat lehet kezelni a bűnmegelőzés, bűnüldözés és az igazságszolgáltatás intézményrendszerének mű-

ködtetéséhez. Továbbá társadalmi szervezetek, egyházak, szakszervezetek, pártok kezelhetnek személyes adatokat a tagság és a tagdíjbefizetések nyilvántartására céljából.

A francia alkotmánytanács[13] foglalkozott azzal a kérdéssel, hogy a faji eredetre vonatkozó állami nyilvántartás létesíthető-e. Az ottani adatvédelmi biztos véleménye az volt, hogy írásos beleegyezés alapján ilyen adatok is nyilvántarthatók. Az adatkezelésre egy az előítéleteket és a társadalmi megkülönböztetést monitorozó kutatási és ellenőrzési rendszer felállítása miatt lett volna szükség. Végül az alkotmánytanács határozata az volt, hogy ilyen adatok még írásos beleegyezés után sem gyűjthetők össze az állampolgárokról. Az alkotmánytanács ehelyett az objektív *születési hely* adat kezelését ajánlotta, mivel az nem tartozik a különleges személyes adatok körébe. A francia adatvédelmi biztos ezt személyes kudarcának tekintette.[14]

Definíció szerint az emberi DNS-t tartalmazó biológiai minta (pl. vér, nyál, egyéb testfolyadékok, szövetek) is *személyes* adat. Egyrészt azért, mert személyes azonosítást tesz lehetővé – gondoljunk itt a bűnügyi személyazonosítás módszereire, másrészt pedig azért, mert a DNS tüzetesebb vizsgálatával rendkívül szenzitív, a mintát adó személyhez (sőt annak családjához is) köthető egészségügyi genetikai információt kaphatunk. Tulajdonképpen a fodrásznál lehullott hajszál is személyes adat. Vita van arról az Európai Unióban, hogy az ujjlenyomat vajon különleges személyes adat-e. Ugyanis a személytől származó ujjlenyomatban előfordulhatnak hámsejtek, amelyeket a bűnügyi technika már genetikai személyazonosításra fel tud használni. Ez jelenleg komoly akadályát képezi a vállalati, ujjlenyomatot használó beléptető rendszereknek (mivel a különleges személyes adatok nyilvántartása tilos). Valószínűleg meg kellene különböztetni az ujjlenyomat és az ujjlenyomat-fénykép fogalmát.

Az Avtv. megkülönbözteti az adattörlést és a megsemmisítést egymástól. Utóbbi az adathordozó megsemmisítését is jelenti. A technikai fejlődés indokolta ezt a különbségtételt, mivel a nagy értékű mágneslemezes tároló egységek esetében belátható, hogy az adatok megsemmisítése helyett azok törlése is elegendő, azonos hatású. Nem szükséges a drága mágneslemezt tönkretenni annak érdekében, hogy valamely adatkezelő megszüntesse az adatkezelést.

Az adatvédelemben régi kérdés, hogy az adatok megtekintése adatkezelésnek tekinthető-e, tehát egy illetéktelen betekintés megvalósít-e jogsértést. A definíciókból az látszik, hogy ilyenkor nem a megtekintő tevékenységét kell vizsgálni, hanem az adatkezelő mulasztását (hogy nem zárta ki ezt az illetéktelen személyt az hozzáférésből) ugyanis a harmadik személy számára elérhetővé tétel a 10. pont alapján adattovábbításnak minősül, és ha erre az adatkezelő nem volt jogosult, akkor a jogsértés megállapítható.

A kamerás megfigyelő rendszerek esetén vita van arról, hogy ha *egy közterületen* a képet nem rögzítik, csak egy monitoron figyelik vagyonőrök, akkor az sérti-e a magánélet háborítatlanságát. Erre vonatkozóan van európai bírósági ítélet – az ilyen megfigyelő rendszer egyenrangú azzal, mintha a biztonsági őr (rendőr) a közterületen lenne és megfigyelné

[13] A magyar Alkotmánybíróságnak megfelelő ottani szervezet (http://www.conseil-constitutionnel.fr/), lásd a Wikipédia szócikket.
[14] A francia adatvédelmi biztosnak a parlament számára készített 2007. évi beszámolója (angol nyelvre fordítva).

a tömeget. Ha ez utóbbi nem sért személyiségi jogokat, akkor a kamerás megfigyelés sem.[15]

A definíciók sajnos néhány esetben nem elég pontosak. A *közzététel* például akkor valósul meg, ha *mindenki* számára közzéteszik az adatokat. Ha azonban a harmadik személyek köre korlátozott – bár akár több száz jogosulatlan felhasználó is van köztük – a *közzététel* nem állapítható meg. Tanulságos ebben a tárgyban a Fővárosi Ítélőtábla néhány határozata a pornográf képekkel kapcsolatos bűncselekmény tárgyában. A Büntető Törvénykönyvről szóló 1978. évi IV. törvény (Btk.) 204. § szerint a büntetési tétel 2-8 év, ha a felvételeket nagy nyilvánosság számára hozzáférhetővé teszi az elkövető. A nagy nyilvánosságot a bíróságok a közzététellel azonosítják. A korlátozott körben történő elérhetőség nem azonos a közzététellel.

Az Emberi Jogok Európai Bírósága foglalkozott azzal, hogy a weblapon történő közzététel adattovábbításnak számít-e (tulajdonképpen potenciálisan bárki letöltheti az adatokat). Nagy vita után az a döntés született, – amiben a praktikus szabályozásnak nagy szerepe volt – hogy a közzé tétel nem tekinthető az EU adatvédelmi irányelv szerinti *adattovábbításnak*, mert akkor minden egyes weboldal azonnal jogsértő lenne. Ugyanis az európai adatvédelmi szabályozás nem engedi meg személyes adatok harmadik országba továbbítását csak akkor, ha abban az országban is az európaihoz hasonló, szigorú adatvédelmi szabályok vannak érvényben.

A közérdekű adat, amelyeket az államigazgatás szerveinek közzé kellene tenniük, nem foglal magában személyes adatokat. Azonban a (köz)hivatali beosztással összefüggésben kiadott dokumentumok pl. engedélyek, határozatok, szerződések, állásfoglalások aláírásai között szereplő név, beosztás, dátum, aláírás, intézmény megnevezése és címe közérdekű adat. Ugyanakkor a címzettek, kérelmezők, engedélyesek, szerződő felek stb. adatai már általában nem. Közzé tételnél ez utóbbiakat ki kell takarni a szövegből. A törvény a közpénz felhasználásával kötött nagy értékű vállalkozási szerződések teljes formáját, minden adatával együtt, közérdekű adatnak nyilvánította, és ezeket közzé is kell tenni.

2.1. Egyéb törvényekben található meghatározások

Az elektronikus információszabadságról szóló 2005. évi XC. törvényben található definíciók

> a) adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
>
> b) adatközlő: az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;
>
> c) közzététel: az e törvényben meghatározott adatoknak internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, ki-

[15] Perry – Egyesült Királyság ügy ítélete, Emberi Jogok Európai Bírósága, 2003. július 17. 40. § (No. 63737/00). Magyarországon közterületen kamerás megfigyelést csak a rendőrség vagy a közterület felügyelet végezhet, azaz egy szigorúbb szabályozás van érvényben.

nyomtatható és részleteiben is kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen történő hozzáférhetővé tétele.

Az elektronikus információszabadságról szóló törvény definíciói az elmúlt időszakban kisebb mértékben megváltoztak. Az egyik kérdés az volt, hogy a közzététel jelenti-e azt, hogy a közzétett dokumentumot a letöltő felhasználó szabadon használhatja-e. Korábban a Magyar Közlöny állományai védett PDF formátumban kerültek az Internetre, amelyekből nem lehetett részleteket kimásolni. A törvény végül úgy változott meg, hogy a PDF állományból ki is másolhatók szövegrészek. Ez lehetővé teszi azt, hogy rosszhiszeműen manipulálják a jogi szövegeket. A védelmet ez ellen az biztosítja, hogy a közhiteles verzióhoz mindenki korlátozás nélkül fér hozzá, és így a visszaélések megakadályozhatók.

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvényben található definíciók

a) egészségügyi adat: az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátó hálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás);

b) személyazonosító adat: a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel (a továbbiakban: TAJ szám) együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására;

c) gyógykezelés: minden olyan tevékenység, amely az egészség megőrzésére, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógyítása, a megbetegedés következtében kialakult állapotromlás szinten tartása vagy javítása céljából az érintett közvetlen vizsgálatára, kezelésére, ápolására, orvosi rehabilitációjára, illetve mindezek érdekében az érintett vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerek, gyógyászati segédeszközök, gyógyászati ellátások kiszolgálását, a mentést és betegszállítást, valamint a szülészeti ellátást is;

d) orvosi titok: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat;

e) egészségügyi dokumentáció: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától;

f) kezelést végző orvos: az érintett gyógykezelését végző vagy abban közreműködő orvos;

g) betegellátó: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész;

> h) [törölve]
>
> i) adatkezelő: a betegellátó; az intézményvezető; az adatvédelmi felelős; továbbá közegészségügyi-járványügyi közérdekből az 5. § (3) bekezdésében meghatározott szervek és személyek; továbbá a 22. § szerinti esetekben az ott meghatározottak szerint az egészségbiztosítási szerv; a 22/E. §-ban meghatározottak szerint az orvosszakértői, rehabilitációs, illetve szociális szakértői szerv; a Nyugdíj-biztosítási Alap kezeléséért felelős nyugdíj-biztosítási szerv és a nyugdíj-biztosítási igazgatási szerv; továbbá a 16/A. §-ban meghatározottak szerint, valamint a lakossági célzott szűrővizsgálatok szervezése érdekében a 3. § b) pont szerinti személyazonosító adat tekintetében az egészségügyi államigazgatási szerv; a 14/A. §-ban meghatározott adatok tekintetében a gyógyszer, gyógyászati segédeszköz, gyógyászati ellátás kiszolgáltatója, illetve nyújtója; a 15/A. §-ban meghatározattak szerint a munkavédelmi hatóság és a tevékenységének ellátását segítő munkahigiénés és foglalkozás-egészségügyi szerv;
>
> j) közeli hozzátartozó: a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs;

A személyes egészségügyi adat definíciójával két probléma is felmerül. A Magyar Köztársaság Alkotmánybírósága foglalkozott azzal a kérdéssel, hogy a személyes adatok jelenlegi felosztása: miszerint vannak a *normál* és vannak a *különleges* személyes adatok elegendő-e, vagy indokolt lenne újabb kategóriákat bevezetni. A kérdés annak kapcsán merült fel, hogy az egészségügyi adatok korábbi definíciója tartalmazta a szexuális életre vonatkozó adatokat is, amennyiben ilyenekre a gyógykezeléshez szükség van. A 65/2002.(XII. 3.) számú AB határozat nem volt egyhangú, több bíró is különvéleményt csatolt hozzá. A többségi szavazással meghozott döntés után azonban az AB törölte a szexuális szokásokra vonatkozó adatokat az Eüaktv. 3. § a) pontjából. Ezzel megállapította, hogy a különleges személyes adatokon belül még van egy védettebb adatcsoport is. Az ellenvélemények egy része arra irányult, hogy a különleges személyes adat már egy eleve sokkal határozottabb védelmet jelent, és nincs szükség erre az új kategóriára. Az alkotmánybírók többsége azonban észrevette azt a még ma sem megoldott kérdést, hogy milyen esetekben engedhető meg az egészségügyi adatok (önmagukban is igen szenzitív személyes adatok) törvényben előírt kényszerű kezelése. Az Eüaktv.-ben felsorolt mintegy negyven célból történő kényszerű adatkezelés alkotmányosan megengedhető-e egyáltalán?

Jelenleg Magyarországon az egészségügyi adatok definíciójában az is megoldatlan kérdés, hogy a társadalombiztosítási elszámolás érdekében továbbított személyes adatok egészségügyi adatnak minősülnek-e egyáltalán, mert akkor indokolt lenne nagyobb védelemben részesíteni őket. Az Egészségügyi Minisztérium úgy tartja, hogy ezek az adatok nem tartoznak a különleges személyes adatok közé, és így is viselkedik, amikor az adatkezeléssel kapcsolatos jogszabályokat alkotja. Ezzel szemben áll az Európai Bizottság ún. 29. cikk alapján létrejött – adatvédelmi – munkacsoportjának a véleménye a személyes adat és személyes egészségügyi adat fogalmáról[16], amely az utóbbiba az igénybevételre vonatkozó adatokat is egyértelműen besorolja. Amióta 2006-ban megváltozott az Eüaktv. és a társadalombiztosítás a BNO (Betegségek Nemzetközi Osztályozása) kódokat[17] is összegyűjti

[16] WP131 számú munkadokumentum az elektronikus egészségügyi nyilvántartásban (EHR) tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról

[17] Egy nyilvános BNO kereső szolgáltatás: http://www.gyogyinfok.hu/forum/BNO/index.asp

minden egyes ellátásról – az adatok már egyértelműen a különleges személyes adatok közé tartoznak. Az utóbbi időben azonban felmerült, hogy egyes egészségre utaló, kis szenzitivitású adatokat pl. optometriai adatok (szemüveg), munkaköri alkalmasság ténye (alkalmas/nem alkalmas valaki egy adott munkakörre) kivegyenek ebből a körből.[18]

A definíciók között az i) pontban található meg az adatkezelő meghatározása. Láthatjuk, hogy a kezelőorvoson kívül még kik, hány különböző jogcímen tekinthetnek be ellátási dokumentációkba.

A humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvényben található definíciók

> a) érintett: genetikai mintát szolgáltató, az e törvény szerinti adatkezelővel kapcsolatba került vagy kerülő természetes személy;
>
> b) genetikai minta: minden, e törvény szerinti humángenetikai vizsgálat, illetve humángenetikai kutatás céljából levett, vagy e törvény keretei között e célra egyébként felhasználni kívánt, emberből származó biológiai anyagminta (szövet-, sejt-, testnedvminta, transzformált sejtvonal vagy sejtekből kivont DNS, RNS);
>
> c) genetikai adat: meghatározott érintett személy örökletes tulajdonságaira vonatkozó olyan információ, amely genetikai minta feldolgozásából, illetve az egészségügyi dokumentációból származik, és amely az egyén genetikai eredetű betegségekkel kapcsolatos kockázatára, örökölt hajlamára, testi vagy viselkedésbeli jellemzőire utal, és alkalmas lehet arra, hogy az egyén azonosítható legyen;
>
> d) kódolt genetikai minta vagy adat: olyan genetikai minta vagy adat, amely mellett a mintát szolgáltató személyre vonatkozó összes személyazonosító adatot kóddal helyettesítették;
>
> e) pszeudonimizált genetikai minta vagy adat: olyan kódolt genetikai minta vagy adat, amelynél a személyazonosító adatot helyettesítő kódot az érintett személy kizárólagos rendelkezésére bocsátották;
>
> f) anonimizált genetikai minta vagy adat: olyan genetikai minta vagy adat, amellyel kapcsolatban az érintettre vonatkozó összes személyazonosító adatot személyazonosításra alkalmatlanná tettek;
>
> g) biobank: genetikai mintát és az ehhez kapcsolódó genetikai és személyazonosító adatokat az e törvény szerinti humángenetikai vizsgálat, illetve humángenetikai kutatás céljából tartalmazó mintagyűjtemény.

A 2008-ban elfogadott humángenetikai törvény jelentősen eltér a 2004-es törvényjavaslattól. A legfontosabb változás a biológiai minta és a nyert genetikai adat megsemmisítéséhez/törléséhez való jog. A korábbi elképzelések szerint az adattárolás kényszerített lett volna, azonban ennek tarthatatlanságát a jogalkotó felismerte és helyesbítette a törvényt. A

[18] A luxemburgi Európai Bíróságnak (ECJ) a C-101/01. sz. Bodil Lindqvist-ügyben 2003. november 6-án hozott ítélete szerint: az, hogy valakinek megsérült a lábfeje, és ezért orvosi indokból csak részmunkaidőben dolgozik, az európai adatvédelmi irányelv 8. cikkének (1) bekezdése értelmében egészségi állapotra vonatkozó személyes adatnak minősül.

törvénnyel szemben megfogalmazott kritikák szerint a hiányosságok közé tartozik, hogy a törvény nem tiltja meg egyértelműen a biztosítók és munkaadók számára a genetikai információhoz történő hozzájutást. A törvény megsértése esetén nincs lehetőség jogorvoslatra, a vétkesek szankcionálására. A törvény még mindig lehetővé teszi, hogy genetikai mintához lehessen jutni az érintettek tájékoztatása nélkül – a más célból adott szövetminta megszerzésével. Etikailag komolyan kifogásolható az is, hogy a törvény hatályba lépésével egyidejűleg a Parlament módosította az Eütv. 211-214. §-ának szövegét és szabaddá tette a halottakból történő szövetkivételt orvosi kutatás céljából a hozzátartozók tájékoztatása és beleegyezése nélkül, ha az elhalt személy életében ez ellen nem tiltakozott. Az állampolgári jogok biztosa 2010-ben kifogásolta a jelenlegi gyakorlatot.

A Büntető Törvénykönyvről szóló 1978. évi IV. törvény néhány adatvédelmi tárgyú paragrafusa

173/D. §
(1) Aki emberen orvostudományi kutatást engedély nélkül, vagy az engedélytől eltérően végez, bűntettet követ el, és öt évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés alkalmazásában engedély alatt az egészségügyről, illetőleg az emberi felhasználásra szánt gyógyszerekről szóló törvényben meghatározott engedélyt kell érteni.

177/A. §
(1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével jogtalan haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel,
b) az adatok biztonságát szolgáló intézkedést elmulasztja,

vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.
(3) A büntetés vétség miatt két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges személyes adatra követik el.
(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

177/B. §
(1) Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével

a) tájékoztatási kötelezettségének nem tesz eleget,
b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít,
c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz,

vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt jogtalan haszonszerzés végett követik el.

Az itt látható paragrafusok tárgyalják a személyes adatok védelmével kapcsolatos büntetőjogi tényállásokat és büntetési tételeiket. A 177/A. §-ban szereplő „*jelentős érdeksérelmet okozva*" megszorítást a büntetőjogban jelentős értékre történő elkövetésként interpretálják, ami a Btk. 138/A. §-a szerint 2-50 millió forint értékű kárként van definiálva. Ezért gyakorlatilag kizárt az, hogy személyes adattal elkövetett jogsértés esetén a bíróság valakinél ezt a *vétséget* megállapítsa. Ehhez ugyanis egyértelműen bizonyítani kellene egy ekkora mértékű károkozást. Az adatvédelmi jogszabályok megsértésével okozott kár rendszerint nem vagyoni jellegű, sokkal inkább az emberi méltóságot sérti. A Polgári Törvénykönyvről szóló 1959. évi IV. törvény (Ptk.) a károkozásokat vagyoni és nem vagyoni károkozásra bontja. Az emberi méltóság megsértése esetén a nem vagyoni kár megtérítése érdekében pert lehet indítani. A Legfelsőbb Bíróság azonban más perek tanulságai alapján a nem vagyoni kárnak egy olyan definícióját tette közzé (az egyént akkor éri nem vagyoni kár, ha nem tudja előző életét a társadalomban tovább folytatni, vagy az jelentősen megnehezül), amely lényegében kizárta azt, hogy adatvédelemhez fűződő jog megsértése esetén nem vagyoni kárigénnyel sikeresen lehessen fellépni. Az új Polgári Törvénykönyv a tervek szerint be fogja vezetni a *sérelemdíj* fogalmát, amelyet az emberi méltóság megsértése esetén lehet megítélni. Ez lesz az a lehetőség, amely alkalmas lehet a károkozás jóvátételére. A Btk. 177/A. §-ába 2009-ben Dr. Jóri András, adatvédelmi biztos javaslatára került be az *anyagi haszonszerzés* motiváció.

Ellenőrző kérdések

1. Milyen adatokat nevezünk személyes adatnak?
2. Mik a különleges személyes adatok?
3. Mi az adatkezelés definíciója?
4. Mi az adattovábbítás definíciója?
5. Mely adatokat nevezünk egészségügyi személyes adatoknak?
6. Mi az adattörlés és az adatmegsemmisítés közötti különbség?
7. Személyes adat-e a nyál?
8. Adattovábbítás-e a weblapon történő közzététel?
9. Soroljon fel néhány adatkezelőt, aki a kezelőorvoson kívül még megismerhet egészségügyi személyes adatot?
10. Milyen rendelkezéseket hiányolnak a humángenetikai törvényből?
11. A Büntető törvénykönyv mely szakasza tartalmazza az adatvédelmi vétségeket, bűncselekményeket?
12. Hogyan interpretálják a *jelentős érdeksérelem* kifejezést a bíróságok?

3. Kapcsolódó nemzetközi dokumentumok

A magánélet és ezen belül a személyes adatok védelmével több nemzetközi dokumentum is foglalkozik. Tekintsünk át először néhány általános emberi jogi dokumentumot. Ezek fontos jellemzője, hogy jogilag nem kötelezik az aláíró államokat, legfeljebb irányadók a számukra.

3.1. Általános emberi jogi dokumentumok

Az Egyesült Nemzetek Szervezete (ENSZ) 1948-ban fogadta el Az Emberi jogok egyetemes nyilatkozatát. Ennek 12. cikke így szól: '*Senkinek a magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez*'.[19]

Később az ENSZ tagállamok kezdeményezték ennek a nyilatkozatnak a pontosítását és készítettek egy nemzetközi egyezményt. Ez tovább részletezi az Emberi jogok egyetemes nyilatkozatában felsorolt polgári és politikai jogokat és szabadságokat. Az egyezményt az Egyesült Nemzetek Szervezetének Közgyűlése fogadta el 1966. december 16-án, és 1976. március 23-án lépett hatályba. 2001 végéig az egyezményt 147 állam erősítette meg, Magyarország az aláírók között szerepel, így rá nézve ez kötelező jogi erővel is bír.

A Polgári és politikai jogok nemzetközi egyezségokmányának 17. cikke szerint: '*Senkit sem lehet alávetni a magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig a becsülete és jó hírneve elleni jogtalan támadásnak. Ilyen beavatkozás vagy támadás ellen mindenkinek joga van a törvény védelmére*'.[20]

A világ legfejlettebb országait tömörítő OECD (Organization for Economic Co-operation and Development, Gazdasági Együttműködési és Fejlesztési Szervezet) 1960-ban alakult, a korábbi OEEC (Organization for European Economic Co-operation) jogutódjaként. Kezdetben 20 alapító tagja volt, később azonban új tagokat vett fel. Magyarország 1996-ban lett a szervezet 27. tagállama. Az OECD 1980-ban egy útmutatót adott ki a magánélet és a határokon keresztül továbbított személyes adatok védelmével kapcsolatban.[21] Az útmutató az OECD tanácsának ajánlása a tagállamok számára amely az OECD három fő célkitűzését hivatott alátámasztani: többpárti demokráciát, az emberi jogok tiszteletben tartását, és a szabad piacgazdaságot.

Az ajánlás létrejöttét az indokolta, hogy a tagországok közül több is elkezdett adatvédelmi törvényeket készíteni, amelyek azonban nehezen voltak összeegyeztethetők. Az ajánlás alapelveket fektetett le, jogi kötelezettség nélkül. Ilyenek voltak például az adatkezelés átláthatósága (traszparencia); az adatkezelés célhoz kötöttsége, korlátozottsága; a tisztességes adatkezelés, az érintettek személyes részvétele: tájékoztatás az adatkezelés tényéről, másolat biztosítása a kezelt személyes adatokról, az adatok kijavításához és törléséhez való jog, az adatkezelés alapja az érintett beleegyezése vagy törvényi rendelkezés;

[19] Az ENSZ Emberi Jogi Főbiztos irodájának honlapján megtekinthető magyar nyelven.
[20] A Magyar ENSZ Társaság honlapján megtekinthető a nemzetközi szerződés szövege.
[21] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

illetve az adatkezelés biztonságossága. Az ajánlás megengedte, hogy az államok kivételeket tegyenek, és egyes adatkezeléseket kivonjanak az ajánlás hatálya alól. A dokumentum azonban megkövetelte a kivételek nyilvánosságra hozását. Az adatok szenzitivitásának mérlegelését az államokra bízta mondván, hogy ezen a téren nagyok az eltérések az egyes országok között.

A Német Szövetségi Köztársaság alkotmánybíróságának 1983. decemberi ítélete[22] a népszámlálással kapcsolatban (Volkszahlungsurteil) ugyancsak fontos nemzetközi dokumentumnak tekinthető. A német alkotmánybíróság alkotmányellenesnek minősítette és ezért megsemmisítette a népszavazásról szóló törvény néhány részletét. Ennél is fontosabb azonban az ítéletnek az az általános megállapítása, hogy „*az (emberi méltósághoz és a személyiség szabad kibontakoztatásához való) alapjog biztosítja az egyénnek azt a jogát, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról*”. Ez a rövid mondat később számos további ítélet alapja lett. Például, a magyar Alkotmánybíróság 15/1991. számú határozatának meghozatalában is jelentős szerepet játszott. Jogi dokumentumban ekkor jelent meg először az információs önrendelkezés tartalmára vonatkozó megállapítás.[23]

3.2. Az Európai Unió dokumentumai

Az alább ismertetésre kerülő dokumentumok alapvető szerepet töltenek be az Európai Unió tagállamainak életében. Az első három dokumentum az Európa Tanács (Council of Europe)[24] által létrehozott nemzetközi egyezmény. Az Európa Tanács egy, az Európai Uniótól független nemzetközi szervezet. Az általa létrehozott nemzetközi egyezményekhez az államok szabadon csatlakozhatnak. Számos Európán kívüli ország is megtalálható az aláíró államok között, pl. Dél-Amerikából. Az egyezmények formailag többoldalú nemzetközi egyezmények, amelyeket független államok egymással kötnek, az Európa Tanács a mediátor, a tárgyaló szerepét vállalja. A csatlakozás nem kötelező, de nem lehet az Európai Unió tagja olyan állam, amely néhány alapvető nemzetközi egyezmény betartására nem vállalt kötelezettséget. A Római és a Strasbourgi Egyezmények az EU alapvető egyezményei, tehát ezeket minden tagállamnak el kell fogadnia. Az Ovideoi Egyezmény esetében a tagállamok megosztottak ma is, többen tartózkodnak az aláírásától. Magyarország mind a három egyezményt aláírta és a Parlament jóváhagyása után törvény formájában hatályba is léptek.

Az Európa Tanács 1949-ben jött létre, 10 alapító állam kezdeményezésére a II. világháború utáni rendezés, az újjáépítés elősegítésére. Később a szerepe a természeti kincsek közös kihasználására, a jobb munkakörülmények biztosítására, illetve az alapvető emberi jogok védelmére módosult. A legelső nemzetközi egyezmények egyike volt az 1950-ben Rómában aláírt Emberi jogok európai egyezménye (EJEE) az emberi jogok és az alapvető szabadságjogok védelméről.[25] Magyarországon az egyezményt az emberi jogok és az alap-

[22] 15.12.1983 ügyszám: 1 BvR 209, 269, 362, 420, 440, 484/83.
[23] Dr. Majtényi László: Az információs szabadságjogok, Complex Kiadó Kft. 2006. 79-80. oldal
[24] Az Európa Tanács (Council of Europe) nem keverendő össze az Európai Tanáccsal (European Council). Az előbbi egy az Európai Uniótól független nemzetközi szervezet, az utóbbi pedig az EU tagállamok kormányfőinek és az Európai Bizottság elnökének tanácsa.
[25] Az Európa Tanács egyezménytárában az ETS-005 számú egyezményt kell keresni, angol neve: ECHR, European Convention on Human Rights.

vető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről szóló 1993. évi XXXI. törvény hirdette ki, amelyet 1993. február 1-től kell alkalmazni. Az egyezmény szól pl. a halálbüntetés tilalmáról, de a tisztességes tárgyaláshoz való jogról, a hatékony jogorvoslathoz fűződő jogról, a szólás- és vallásszabadságról stb. Az EJEE 8. cikke foglalkozik a magánélet védelmével:

'*1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.*'

Az EJEE 8. cikkben biztosított, a magánélet tiszteletben tartásához fűződő jogot korlátozni lehet a 2. pontban felsorolt indokokkal és esetekben. Az EJEE-vel történő kompatibilitás megőrzése érdekében, a magánéletbe történő beavatkozásnak bizonyos feltételeket kell kielégítenie. Egyrészt törvényekkel összhangban kell, hogy történjen, másrészt szükségesnek kell lennie egy demokratikus társadalomban. Ez azt jelenti, hogy a beavatkozásnak meg kell felelnie mind a *fontos társadalmi igény*, illetve *az elérni kívánt jogos céllal való arányosság* feltételének. Az ilyen jogos célokat kimerítően felsorolja a 8. cikk 2. pontja.

Az EJEE hozta létre a strasbourgi székhelyű Emberi Jogok Európai Bíróságát (EJEB) . Ennek a bíróságnak a feladata az, hogy az egyezményben biztosított emberi jogok betartását biztosítsa. Az aláíró országokból bármely állampolgár fordulhat vitás kérdések eldöntése érdekében a bírósághoz. A pert formálisan a saját országa ellen kell indítsa azért, mert az nem biztosítja számára az egyezményben deklarált jogait. A bíróság elvi döntéseket hoz személyes képviselet nélkül, a felekkel csak írásban kommunikál. A per teljesen ingyenes – azonban hosszabb ideig is eltarthat.

Az EJEB döntései azt mutatják, hogy az EJEE nem ad abszolút garanciát a személyes adatok bizalmasságára, mert nem minden adatkezelést tekintenek a magánélet megzavarásának, ezért az Európa Tanács 1981-ben létrehozta az Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során nevet viselő nemzetközi egyezményét.[26] Ez az adatvédelmi egyezmény volt az első nemzetközi jogi kötelezettséget jelentő dokumentum a személyes adatok bizalmas kezelésével kapcsolatban. Magyarországon az egyezményt az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény hirdette ki és 1998. február 1-jétől kell alkalmazni.

Az egyezmény minden gépi személyes adatállományra és a személyes adatok gépi feldolgozására vonatkozik mind a köz- mind pedig a magánszférában (3. cikk)[27] mindaddig, amíg az adatok egy azonosított vagy azonosítható személlyel kapcsolatba hozhatók (2. cikk), függetlenül a nemzetiségüktől vagy a lakóhelyüktől. Az egyezményhez fűzött magyarázat szerint az *érintett személy* az egyezményben azt az alapelvet fejezi ki, hogy ennek a személyeknek **alanyi joga** van a rá vonatkozó tárolt személyes információkhoz, még ha

[26] Az Európa Tanács egyezménytárában az ETS-108 számú egyezményt kell keresni.
[27] Az aláíró országok vállalhatták, hogy manuális (pl. papír alapú) adatállományokra is alkalmazzák. Magyarország szintén vállalta az egyezmény ilyen kiterjesztését. Lásd a törvény 3. §-át.

mások gyűjtötték is össze azokat. Látható, hogy az OECD irányelv jelentős hatást gyakorolt az egyezmény szövegére.

> 8. Cikk
>
> Az érintettet védő további garanciák
>
> Mindenkinek joga van arra, hogy
>
> a) tudomást szerezzen a személyes adatok automatizált állományáról, annak fő céljairól, valamint az adatállományt kezelő személyéről és szokásos lakhelyéről vagy székhelyéről;
>
> b) ésszerű időközönként és túlzott késedelem vagy költség nélkül értesüljön arról, hogy egy automatizált adatállományban személyes adatait tárolják-e, és ezekről az adatokról számára érthető formában tájékoztassák;
>
> c) indokolt esetben ezeket az adatokat helyesbíttethesse vagy töröltethesse, ha ezen adatok feldolgozása ellentétes a jelen Egyezmény 5. és 6. Cikkében foglalt alapelveket érvényesítő hazai jog rendelkezéseivel;
>
> d) jogorvoslattal élhessen, ha e Cikk b) és c) pontjában foglalt tájékoztatási vagy indokolt esetben közlési, helyesbítési, illetve törlési kérelmét nem teljesítik.[28]

Az Európa Tanács 1997-ben hozta létre az Egyezmény az emberi lény emberi jogainak és méltóságának védelméről a biológia és az orvostudomány alkalmazására tekintettel nevet viselő nemzetközi egyezményét.[29] Az egyezmény több olyan jogot kibővít, amelyet már az EJEE tartalmazott és kidolgozta hogyan kell ezeket alkalmazni az orvostudomány területére. Az EJEE-vel ellentétben, amelyet minden EU tagállam aláírt, az Emberi jogokról és a biomedicináról szóló egyezményt több tagállam nem írta alá, pl. Egyesült Királyság, Franciaország, Németország. Annak ellenére, hogy az egyezmény nem vonatkozik közvetlenül több EU tagállamra, mindazonáltal jelentős abból a szempontból, hogy az EJEB felhasználta, amikor ítéletet hozott olyan országokkal szemben, amelyek nem tagjai az egyezménynek. Magyarországon az egyezményt az Európa Tanácsnak az emberi lény emberi jogainak és méltóságának a biológia és az orvostudomány alkalmazására tekintettel történő védelméről szóló, Oviedóban, 1997. április 4-én kelt Egyezménye: Az emberi jogokról és a biomedicináról szóló Egyezmény, valamint az Egyezménynek az emberi lény klónozásának tilalmáról szóló, Párizsban, 1998. január 12-én kelt Kiegészítő Jegyzőkönyve kihirdetéséről szóló 2002. évi VI. törvény hirdette ki és 2002. május 1-jétől kell alkalmazni. Az egyezmény 10. cikkelye szerint:

1. Mindenkinek joga van ahhoz, hogy magánéletét tiszteletben tartsák a róla szóló egészségügyi adataival kapcsolatban.

2. Mindenkinek joga van tudni bármilyen információról, amelyet az egészségével kapcsolatban gyűjtöttek össze. Azonban a pácienseknek azt a kívánságát, hogy ne tájékoztassák őket ugyancsak figyelembe kell venni.

3. Kivételes esetekben a 2. pontban szereplő jog érvényesítése törvénnyel korlátozható a páciens érdekében.

[28] Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény

[29] Az Európa Tanács egyezménytárában a CETS-164 számú egyezményt kell keresni.

Az Európa Tanács 1999-ben javasolta, hogy hozzák létre az Európai Unió emberi jogainak egy aktuális jegyzékét. Az elkészült dokumentumot 2000-ben Nizzában mutatták be, de sokáig nem volt biztos a státusza. A benne felsorolt emberi jogokat a Római Egyezményből, továbbá az EJEB és a luxemburgi Európai Bíróság ítéletei alapján gyűjtötték össze.[30] Az Alapvető jogok chartája két cikke hangsúlyozza a magánélet védelmének fontosságát: a 7. cikk szerint: '*Mindenkinek joga van ahhoz, hogy tiszteletben tartsák magánéletét, családi életét, otthonát és kapcsolattartását.*' A 8. cikk szerint: '*1. Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. 2. Az ilyen adatokat tisztességesen kell feldolgozni meghatározott célokból az érintett személy beleegyezése alapján vagy valamilyen törvényben lefektetett jog alapján. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokhoz hozzáférjen, és joga van azokat kijavíttatni. 3. E szabályok betartása felett független hatóság őrködik.*'

Az Alapvető jogok chartája végül 2009. december 1-jén törvényerőre emelkedett, mivel a 25 EU tagállam mindegyike megerősítette aláírásával és nemzeti törvényben kihirdette. A közeljövőben a charta fontos szerepet fog betölteni az unió életében és meghatározza a jogalkotás további folyamatát.

3.3. Az Európai Parlament és a Miniszterek Tanácsának 95/46/EK számú adatvédelmi irányelve

Az Európai Unióban sokáig nem volt egységes adatvédelmi szabályozás és a tagállamok maguk hoztak létre adatvédelmi törvényeket. Igaz, hogy minden tagállam aláírója volt a Római Egyezménynek (EJEE) , azonban az csak implicit módon foglalta magába a személyes adatok védelmét. Az egyezmény 8. cikke a magán- és családi élet védelmét, valamint a levelezés tiszteletben tartását tartalmazta. Az 1981-es Strasbourgi Egyezmény az érintettek alapvető, alanyi jogait definiálta a rájuk vonatkozó adatokhoz és alapvető célja a tagállamok közötti akadálymentes és biztonságos adatcsere biztosítása volt.

A tagállamok ezektől az egyezményektől függetlenül saját adatvédelmi törvényeket alkottak. Annak érdekében, hogy ezek a törvények a lehető legjobban hasonlítsanak egymáshoz, azonos jogokat és jogintézményeket tartalmazzanak az Európai Parlament egy adatvédelmi irányelvet dolgozott ki. Ez minden tagállamot arra kötelez, hogy az ajánlás alapján, azzal harmonizáló nemzeti adatvédelmi törvényt hozzon létre. Az Európai Parlament megvizsgálja a nemzeti adatvédelmi törvényt, és határozatot hoz arról, hogy az adott nemzet adatvédelmi törvénye kompatibilis-e az adatvédelmi irányelvvel. A pontos megnevezése: Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az adatvédelmi irányelv megjelent magyar nyelven az Európai Unió hivatalos lapjában (Hivatalos Lap L 281, 23/11/1995 31–50. oldal) .

A magyar adatvédelmi törvényt – mivel azt korábban már elfogadta a magyar Parlament – többször is módosítani kellett, hogy meg tudjon felelni az adatvédelmi irányelvnek. Az Európai Közösség Bizottsága 2000. július 26-án meghozta 2000/519/EK számú döntését arról, hogy Magyarország az adatvédelmi irányelv alapján létrehozott nemzeti adatvédelmi törvényével biztosítja az egyének megfelelő védelmét. Ez a határozat is az Európai Unió hivatalos lapjában megjelent (Hivatalos Lap L 215, 25/8/2000 4–6. oldal).

[30] Magyar fordításban megjelent az Európai Unió hivatalos közlönyének, 2000/C 364/01 számában.

Az Európai Unió adatvédelmi irányelvének megalkotására jelentős hatást gyakorolt a francia adatvédelmi törvény: az n°1978-17 számú törvény (1978. január 6.) az adatfeldolgozásról, az adatállományokról és a személyes szabadságról, amelyet módosított a 2004. augusztus 6-án elfogadott törvény az egyének védelméről személyes adataik feldolgozása során, lásd. (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data). A francia adatvédelmi törvény eredeti, francia nyelven letölthető, továbbá angol fordításban is letölthető a francia adatvédelmi bizottság honlapjáról.

A német szövetségi adatvédelmi törvény 2009. szeptember 1-jén elfogadott módosításokkal egyesített szövege (Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003, Federal Law Gazette I, p. 66, last amended by Article 1 of the Act of 14 August 2009., Federal Law Gazette I, p. 2814), in force from 1 September 2009) eredeti német nyelven letölthető, valamint angol fordításban letölthető a német szövetségi adatvédelmi biztos honlapjáról. Az Európai Unió egyes tagállamai pl. Egyesült Királyság, Dánia[31], Olaszország[32] stb. az irányelv megjelenése után új adatvédelmi törvényeket hoztak létre. Ezek természetesen összhangban vannak az irányelv szövegével, fejezet struktúrájával, jogi fogalmaival – fel sem merülhet, hogy ne lennének kompatibilisek az irányelvvel. Az Egyesült Királyság új, a korábbi 1990-es törvényt felváltó adatvédelmi törvénye 1998-ban jelent meg (Data Protection Act 1998), letölthető az Egyesült Királyság jogi archívumából.

Az irányelv először ismerteti a megalkotásának célját, a definíciókat. A 6. cikke az adatkezelés nyolc fontos feltételét definiálta. Ezek minden egyes adatkezelés esetén, együttesen kell, hogy fennálljanak:

1. az adatkezelés tisztességes és törvényes
2. az adatkezelés előre meghatározott, kifejezett és törvényes célból történik
3. ez előre megadott célokkal inkompatibilis módon nem dolgozzák tovább fel őket; történeti, statisztikai és tudományos célú feldolgozás nem tekinthető inkompatibilisnek, amennyiben a tagállamok megfelelő védelmi intézkedéseket hoznak
4. az adatok mennyisége adekvát, releváns, és nem túlzott
5. az adatok pontosak, és ha szükséges naprakészek is
6. olyan formában tárolják őket, hogy az érintettek azonosítását nem teszik lehetővé hosszabb ideig, mint szükséges
7. az érintettek hozzáférhetnek, kérhetik a korrekciójukat és törlésüket
8. biztonságos körülmények között tárolják őket

Jelentős eltérés mutatkozik az irányelv 7. cikke és a magyar adatvédelmi törvény között. Az irányelv hat esetet különböztet meg, amely esetekben a személyes adatok feldolgozhatók. A magyar Avtv. ezzel szemben, ezek közül csak három esetet engedélyez [az a), c), és a d) pontokat].

> A tagállamok rendelkeznek arról, hogy a személyes adatok csak abban az esetben dolgozhatók fel, ha:
> a) az érintett ahhoz egyértelmű hozzájárulását adta; vagy

[31] A 2000-es dán adatvédelmi törvény angol nyelven elolvasható: http://www.datatilsynet.dk/english/
[32] A 2003-as új olasz adatvédelmi törvény, amely felváltotta az 1996-os korábbit angol nyelven elolvasható: http://www.privacy.it/privacycode-en.html

b) az adatfeldolgozás olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy
c) az adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges; vagy
d) feldolgozásuk az érintett létfontosságú érdekei védelméhez szükséges; vagy
e) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges; vagy
f) az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az 1. cikk (1) bekezdése értelmében védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében.

Az irányelv a különleges személyes adatok feldolgozását is több feltételhez köti. Ezek a 8. cikkben vannak felsorolva:

Különleges adatok feldolgozása

(1) A tagállamok *megtilthatják* az olyan személyes adatok feldolgozását, amelyek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkoznak.

(2) Az (1) bekezdést nem alkalmazható abban az esetben, ha:

a) az érintett kifejezett hozzájárulását adta az említett adatok feldolgozásához, kivéve, ha a tagállam joga úgy rendelkezik, hogy az (1) bekezdésben említett tilalom alól nem engedhető kivétel az érintett hozzájárulásával sem, vagy

b) az adatfeldolgozás az adatkezelő kötelezettségei és meghatározott jogai gyakorlása érdekében szükséges a foglalkoztatási jogszabályok területén, amennyiben a megfelelő biztosítékokról rendelkező nemzeti jogszabályok ezt lehetővé teszik, vagy

c) az adatfeldolgozás az érintett vagy más személy létfontosságú érdekeinek védelméhez szükséges abban az esetben, ha az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni, vagy

d) az adatfeldolgozás valamely alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik, politikai, világnézeti, vallási vagy szakszervezeti céllal, azzal a feltétellel, hogy a feldolgozás kizárólag az ilyen szerv tagjaira, vagy olyan személyekre vonatkozik, akik azzal rendszeres kapcsolatban állnak a szerv céljainak megfelelően, és az adatok nem adhatók ki harmadik fél részére az érintettek hozzájárulása nélkül, vagy

e) az adatfeldolgozás olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott, vagy amelyek jogi követelések megállapításához, gyakorlásához vagy védelméhez szükségesek.

(3) Az (1) bekezdés nem alkalmazható, ha az adatok feldolgozása megelőző egészségügyi, orvosi diagnosztikai célból, gondozás vagy feldolgozás alkalmazása vagy egészségügyi szolgáltatások igazgatása céljából szükséges, és ha az adatokat a

nemzeti jog vagy az illetékes nemzeti testületek által meghatározott szakmai titoktartási kötelezettség alá eső egészségügyi szakember vagy azzal egyenértékű titoktartási kötelezettség alá eső más személy dolgozza fel.

(4) Megfelelő garanciák nyújtása mellett a tagállamok, alapvető közérdekből, nemzeti jogszabályaikban vagy a felügyelő hatóság határozatában további mentességeket állapíthatnak meg a (2) bekezdésben foglaltakon kívül.

(5) A bűncselekményekre, büntetőítéletekre vagy biztonsági intézkedésekre vonatkozó adatok feldolgozása kizárólag a hatóság ellenőrzése mellett történhet, vagy ha a nemzeti jog megfelelő külön biztosítékot nyújt, az olyan eltérésekre is figyelemmel, amelyet a tagállamok a megfelelő külön biztosítékot nyújtó nemzeti rendelkezések alapján engedélyezhetnek. Mindazonáltal a büntetőítéletekről teljes körű nyilvántartást csak a hatóság ellenőrzésével lehet vezetni.

A tagállamok rendelkezhetnek arról, hogy a közigazgatási szankciókkal vagy polgári ügyekben hozott határozatokkal kapcsolatos adatokat szintén csak a hatóság ellenőrzésével lehessen feldolgozni.

(6) Az (1) bekezdéstől való, a (4) és (5) bekezdésben említett eltérésekről a Bizottságot értesíteni kell.

(7) A tagállamok határozzák meg a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek feldolgozásának feltételeit.

Az EU adatvédelmi irányelv 28. cikke hozta létre az adatvédelemmel kapcsolatos jogok védelmére hivatott *független hatóságot*. Ennek köszönhetjük az Adatvédelmi Biztosi Hivatal létrejöttét. A 29. cikk pedig létrehozta az európai adatvédelmi biztosok és adatvédelmi szakembereket tömörítő nemzetközi munkacsoportot. Ez a munkacsoport külső szakértőkkel folyamatosan formálja és alakítja az EU adatvédelmi jogát. A munkacsoportot erről nevezték el a 29. cikk alapján létrejött munkacsoportnak. A munkacsoport honlapján nyilvánosságra hozza ajánlásait és dokumentumait először angol nyelven, majd később az EU többi hivatalos nyelvére lefordítva.

Ellenőrző kérdések

1. Miben tér el egymástól a magánélet tiszteletben tartása és a személyes adatok védelméhez való jog?

2. Milyen rendelkezések szerepelnek az ENSZ Egyetemes emberi jogok nyilatkozatában a magánéletről?

3. Milyen előremutató adatvédelmi rendelkezések szerepelnek az OECD 1980-as ajánlásában?

4. Soroljon fel három, az Európa Tanács által létrehozott nemzetközi egyezményt, amely kapcsolatban áll a magánélet védelmével?

5. Miként rendelkezik a Római Egyezmény a magánéletről?

6. Mi a feladata a strasbourgi székhelyű Emberi Jogok Európai Bíróságának?

7. Milyen fontos adatvédelmi rész jogokat biztosít az érintettek számára a Strasbourgi Egyezmény?

8. Mi a témája és lényege az Ovideói Egyezménynek?

9. Mi a jelenlegi státusza az Alapvető jogok chartájának?

10. Mi volt a célja az Európai Parlament és a Tanács által kibocsátott 95/46/EK számú adatvédelmi irányelvnek?

11. Hogyan gondoskodtak a tagállamok az adatvédelmi irányelv megvalósításáról?

12. Nevezzen meg néhány fontos adatvédelmi rendelkezést, amely a 95/46/EK adatvédelmi irányelvben jelent meg először?

4. Fontosabb hazai jogszabályok

A hazai jogszabályok között elsőként az Alkotmánynak a személyes adatok védelmére és a közérdekű adatok nyilvánosságára vonatkozó paragrafusait tekintjük át. Az Alkotmány 8. §-a szerint az alapvető jogok korlátozását minden esetben törvénynek kell szabályoznia, és ez a törvény is csak a szükséges minimális mértékben korlátozhatja az alapvető jogokat, lényeges tartalmukat nem szüntetheti meg. Az személyes adatok védelméhez való jog, illetve az adatvédelmi törvény kétharmados törvénnyé emelése az 59. §-ban található. A közérdekű adatok nyilvánosságáról szól az Alkotmány 61. §-a.

> 8. §
> (1) A Magyar Köztársaság elismeri az ember sérthetetlen és elidegeníthetetlen alapvető jogait, ezek tiszteletben tartása és védelme az állam elsőrendű kötelessége.
> (2) A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg, alapvető jog lényeges tartalmát azonban nem korlátozhatja.
>
> 59. §
> (1) A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a *személyes adatok védelméhez* való jog.
> (2) A személyes adatok védelméről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.
>
> 61. §
> (1) A Magyar Köztársaságban mindenkinek joga van a *véleménynyilvánítás és a szólás szabadságához, továbbá a közérdekű adatok megismeréséhez, valamint terjesztéséhez*.
> (2) A Magyar Köztársaság elismeri és védi a sajtó szabadságát és sokszínűségét.
> (3) A demokratikus közvélemény kialakítása érdekében mindenkinek joga van a megfelelő tájékoztatáshoz a közügyek tekintetében.
> (4) A Magyar Köztársaságban közszolgálati médiaszolgáltatás működik közre a nemzeti önazonosság és az európai identitás, a magyar, valamint a kisebbségi nyelvek és kultúra ápolásában, gazdagításában, a nemzeti összetartozás megerősítésében, illetőleg a nemzeti, etnikai, családi, vallási közösségek igényeinek kielégítésében. A közszolgálati médiaszolgáltatást az Országgyűlés által választott tagokkal működő autonóm közigazgatási hatóság és független tulajdonosi testület felügyeli, céljainak megvalósulása felett pedig az állampolgárok egyes, törvényben meghatározott közösségei őrködnek.
> (5) A közérdekű adatok nyilvánosságáról szóló törvény, valamint a sajtószabadságról és a médiatartalmak alapvető szabályairól rendelkező törvény, továbbá a médiaszolgáltatások felügyeletéről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.

Az Alkotmány paragrafusainak értelmezése, használata és betartatása az Alkotmánybíróság feladata. Az Alkotmánybíróság 1990. óta mond ítéletet a jogszabályok alkotmányosságával kapcsolatban és alkalmazza az Alkotmány paragrafusait. Az Alkotmánybíróságról szóló 1989. évi XXXII. törvény (Abtv.) szerint az AB határozatai mindenkire kötelezőek, ezért az AB úgy tartja, hogy magára a bíróságra is. Ennek következtében saját magát egy-

értelműen precedensbírósággá nyilvánította. Az AB elé tárt indítványok egyik fontos része a korábbi hasonló tárgyban született határozatok feldolgozása.

Az Alkotmánybíróság 15/1991. számú határozata az univerzális személyi szám bevezetését előíró rendelet alkotmányosságát vizsgálta és alapvető megállapításokat tett az információs önrendelkezésről.

> (…) Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy **mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.** Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel a Alkotmány 8. §-ában megkövetelt feltételeknek.
> Bármilyen jogszabály, amely – az alkalmazott eljárásra tekintet nélkül – személyes adat felvételéről, gyűjtéséről, tárolásáról, rendezéséről, továbbadásáról, nyilvánosságra hozásáról, megváltoztatásáról, a tovább felhasználás megakadályozásáról, az adatból új információ előállításáról, vagy akármilyen más módon történő felhasználásáról (a továbbiakban: a személyes adat feldolgozásáról) rendelkezik, **csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adat útját a feldolgozás során követni, és jogait érvényesíteni tudja**. Az erre szolgáló jogintézményeknek tehát biztosítaniuk kell az érintett beleegyezését a feldolgozásba, illetve pontos garanciákat kell tartalmazniuk azokra a kivételes esetekre nézve, amikor az adatfeldolgozás az érintett beleegyezése (esetleg tudta) nélkül történhet. E garanciális jogintézményeknek továbbá – az ellenőrizhetőség érdekében is – objektív korlátok közé kell szorítaniuk az adat útját.
> „Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez az jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. (…) A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, »készletre«, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és tárolás alkotmányellenes.” (ABH 1991, 40, 41-42.)”

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvényt aláírás előtt a köztársasági elnök átküldte az Alkotmánybíróságnak előzetes normakontrollra. Az AB egyes paragrafusokat alkotmányellenesnek talált, és ezért a Parlamentnek meg kellett változtatnia a szöveget. Az Alkotmánybíróság 36/2005. (X. 5.) határozatában az elektronikus megfigyeléssel kapcsolatban leszögezte:

> (…) **A magánszféra lényegi fogalmi eleme éppen az, hogy az érintett akarata ellenére mások oda ne hatolhassanak be, illetőleg be se tekinthessenek.** Ha a nem kívánt betekintés mégis megtörténik, akkor nemcsak önmagában a magánélethez való jog, hanem az emberi méltóság körébe tartozó egyéb jogosultsági elemek, mint pl. az önrendelkezési szabadság vagy a testi- személyi integritáshoz való jog is sérülhet. (ABH, 2005. évi 10. szám)

4.1. A személyes adatok védelméről szóló törvény

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) az Európai Parlament adatvédelmi irányelve által megkövetelt nemzeti adatvédelmi törvény, valamint az Alkotmány 59. §-ában említett személyes adatok adatvédeleméről szóló törvény.

Az adatvédelmi törvény kizárólagosságának alkotmányos védelmét az 1. § (3) bekezdése biztosítja, ugyanis abban az található, hogy az ebben a törvényben foglalt rendelkezésektől eltérni kizárólag akkor lehet, ha azt az Avtv. kifejezetten egy adott adatkezelőre és egy bizonyos adatkezelésre megengedi. Korábban már volt arról szó, hogy az Avtv. módosításához a jelenlévő képviselők kétharmadának igen szavazata szükséges – ez a törvény tartalmát védi az *ad hoc* módosításokkal szemben.

Nemzetközi egyezmény (ETS-108 Strasbourgi Egyezmény) foglalkozott azzal a kérdéssel, hogy mi legyen egy nemzeti adatvédelmi törvény földrajzi hatálya – ebben a kérdésben az aláíró tagállamok a területi hatályt kötötték ki, tehát a Magyar Köztársaság területén folytatott adatkezelésekre ezt a törvényt kell alkalmazni. Ez azt jelenti, hogy a magyar zászló alatt nemzetközi vizeken járó hajón, és a diplomáciai védelem alatt álló külképviseleteken is. Az adatvédelmi törvény nem vonatkozik a személyes célokra gyűjtött és kezelt adatokra pl. telefonregiszterre, e-mail címlistára, fényképekre stb.

Az Avtv. egyik fontos tulajdonsága – amelyről európai szakértők úgy tartják, kiemelkedően szigorú – az, hogy kizárólag akkor engedi meg személyes adatok kezelését, ha azt egy törvény kötelezően előírja, vagy ha az érintett az adatkezeléshez a hozzájárulását megadta. Különleges személyes adatok esetén a hozzájárulásnak írásban kell megtörténnie. Ezeket az alapvető előírásokat az adatvédelmi törvény 3. §-a tartalmazza. Amennyiben az adatkezelést egy törvény elrendeli, akkor annak a törvénynek kellene tartalmaznia a kezelt adatok körét, az adatkezelés célját, a hozzáférések szabályozását, az adatkezelés időtartamát és az adatkezelő személyét. Közérdekből egy törvény elrendelheti személyes adatok nyilvánosságra hozását is, lásd (4) bekezdés. Alapesetben azonban a közérdekű adatok nem foglalhatnak magukban személyes adatokat. Vélelmezni lehet a hozzájárulást az érintett kérelmére induló hivatalos eljárásokban, (6) bekezdés – bár erre a törvény szerint minden esetben fel kellene hívni az érintett figyelmét. A (8) bekezdésében megtalálható az is, hogy az érintett (data subject) vagy más személy életfontosságú érdekében, ha a beleegyezést nem lehetséges megszerezni, akkor hozzájárulás nélkül is lehetséges az adatkezelés. Az életfontosságú érdek, az élethez való alapvető jogból ered, és amennyiben szükséges, katasztrófa helyzetben, balesetben megsérült emberek esetében, életveszély esetén a normál adatvédelmi szabályok nem érvényesek.

> 3. §
> (1) Személyes adat akkor kezelhető, ha
> a) ahhoz az érintett hozzájárul, vagy
> b) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete elrendeli.
>
> (2) Különleges adat akkor kezelhető, ha
> a) az adatkezeléshez az érintett írásban hozzájárul, vagy
> b) a 2. § 2. a) pontjában foglalt adatok esetében, az nemzetközi egyezményen alapul, vagy Alkotmányban biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény elrendeli;
> c) egyéb esetekben azt törvény elrendeli.

(3) Kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

(4) Törvény közérdekből – az adatok körének kifejezett megjelölésével – elrendelheti a személyes adat nyilvánosságra hozatalát. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása, különleges adat esetében írásbeli hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

(5) Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében.

(6) Az érintett kérelmére indult eljárásban a szükséges adatainak kezeléséhez való hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét fel kell hívni.

(7) Az érintett a hozzájárulását az adatkezelővel írásban kötött szerződés keretében is megadhatja a szerződésben foglaltak teljesítése céljából. Ebben az esetben a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából – e törvény alapján – az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbítását, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

(8) Ha az érintett fizikai okból vagy cselekvőképtelensége folytán nem képes hozzájárulását adni adatai kezeléséhez, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint katasztrófa- vagy szükséghelyzet elhárításához vagy megelőzéséhez szükséges mértékben sor kerülhet személyes adatainak, beleértve különleges adatait is, kezelésére.

Az adatvédelmi törvény az Európai Parlament 95/46/EK számú irányelvének megfelelően szabályozza az előzetes tájékoztatás követelményét a 6. §-ában. Eszerint az érintettek számára minden esetben előzetes adatvédelmi tájékoztatást kell adni, amelynek során minden lényeges és fontos ismeretet, közölni kell, beleértve az esetleges jogorvoslati lehetőséget is. A 6. § egy lényeges hibája az, hogy a tájékoztatás megadására kötelezett személy (intézmény) meghatározása a törvényben nem szerepel, hanem ezen a helyen egy általános alany található. A 95/46/EK irányelvben ezzel szemben az szerepel, hogy erre az adatkezelő vagy a megbízottja kötelezett. Amikor nem egyértelmű, hogy kit terhel a tájékoztatási kötelezettség, akkor a törvény általános megfogalmazása miatt, még perrel sem lehet kikényszeríteni a tájékoztatást. A 6. § (3) bekezdése szerint amennyiben az adatkezelést törvény rendeli el egy már meglévő adatállományból, akkor nem szükséges tájékoztatást adni, mert a jogalkotó abból indult ki, hogy az elrendelő törvény minden lényeges információt tartalmaz. Az EU irányelv szerint, ha az adatokat nem az érintettektől szerzik be, az adatkezelőnek akkor is kellene tájékoztatást adnia, ami a magyar törvényből egyszerűen hiányzik.

6. § (1) Az érintettel az adat felvétele előtt közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt is.

(2) Az érintettet – egyértelműen és részletesen – tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

(3) Az adatkezelésről való tájékoztatás megtörténik azzal is, hogy jogszabály rendelkezik a már létező adatkezelésből továbbítással vagy összekapcsolással az adat felvételéről.

(4) A tájékoztatás – különösen statisztikai vagy tudományos (ideértve a történelmi kutatásokat is) célú adatkezelés esetén – megtörténhet az adatgyűjtés tényének, az érintettek körének, az adatgyűjtés céljának, az adatkezelés időtartamának és az adatok megismerhetőségének mindenki számára hozzáférhető módon történő nyilvánosságra hozatalával, ha az egyénre szóló tájékoztatás lehetetlen vagy aránytalan költséggel járna.

Az Európai Parlament adatvédelmi irányelvének 6. cikkéből ismerős adatkezelési alapelvekből tartalmaz hármat az Avtv. 7. §-a. Ugyancsak ez a paragrafus tiltja meg az általános, egységes személyi azonosító jel használatát.

7. § (1) A kezelt személyes adatoknak meg kell felelniük az alábbi követelményeknek:

a) felvételük és kezelésük tisztességes és törvényes;
b) pontosak, teljesek és ha szükséges időszerűek;
c) tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

(2) Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos.

A 8. § a személyes adatok továbbításával és összekapcsolásával, a 9. § a külföldre történő adattovábbítással foglalkozik. Az ETS-108 számú Strasbourgi Egyezmény célja az volt, hogy a csatlakozó államokban (jórészt európai országok) az érintettek jogait, valamint a jogi felelősség és számon kérhetőség azonos szintjét biztosítsák annak érdekében, hogy az egységes belső piac, a szolgáltatások és áruk szabad áramlása megvalósulhasson. A személyes adatok kezelésekor is érvényes az a célkitűzés, hogy egy EU tagállamba történő adattovábbítás belső adattovábbításnak számítson, azaz pontosan olyan szabályoknak kell, hogy megfeleljen mintha az adatátvevő Magyarországon lenne. Ezt fogalmazza meg a 9. § (4) bekezdése. A fizikai adatbiztonság követelményeinek felsorolását tartalmazza a 10. §: (…) *Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak* (…).

Az érintettek alanyi jogait sorolja fel a 11. §. Bárki kérhet utólagos adatvédelmi tájékoztatást, kérheti az adatok kijavítását, ha azok már nem felelnek meg a valóságnak, illetve ha a személyes adatok kezelését nem egy törvény rendelte el kötelezően, akkor az adatok törlését is. Az adatkezelőknek a személyes adatok továbbításáról naplót kell vezetniük. Ebből ki-ki a rá vonatkozó bejegyzéseket is kérheti, azaz megtudhatja, hogy a személyes adatait milyen célból, mikor és hová továbbították. Ha az adatkezelő a beérkezett kérést

nem teljesíti 30 napon belül közérthető módon, írásban, akkor az érintett bírósághoz fordulhat, amely határozattal kötelezi az adatkezelőt a jogos igény végrehajtására.

A 12. § szerint az érintettek másolatot kaphatnak a tárolt adatokról, évente egyszer ingyenesen, valamint visszamenőleges tájékoztatást a kezelt adatok köréről, az adatkezelés céljáról, időtartamáról stb. A korábban megtörtént adattovábbításokról legalább 5 évre (különleges személyes adatoknál legalább 20 évre) visszamenőleg. Ez a tájékoztatás évente egyszer ingyenes, illetve akkor is, ha a tájékoztatás után az adatok helyesbítésére volt szükség, vagy kiderül, hogy azokat jogellenesen kezelték. A 14. § szabályozza az adatok törlésének lehetőségeit. Ha a személyes adatok módosításra kerültek, akkor az adatkezelő **köteles** értesíteni az adattovábbítási napló adatai alapján azokat a további adatkezelőket, akiknél ugyancsak kezdeményezi az adatok kijavítását (15. §). Az érintettek itt felsorolt jogait (másolat a kezelt adatokról, helyesbítés, törlés, utólagos tájékoztatás, adattovábbítási napló részlete) a 16. § szerint törvénnyel korlátozhatják. Az Avtv. szövegébe utólag 2003-ban került be a 16/A. §, amely a tiltakozás jogáról szól. Az EU adatvédelmi irányelv a tiltakozás jogát ennél szélesebb körben biztosítja az érintettek számára. Mivel azonban Magyarországon csak törvénnyel elrendelt (vagy önkéntes hozzájáruláson alapuló) adatkezelés létezik, ahol általában nincs helye a tiltakozásnak, ezért sokáig nem volt miért bevezetni. 2003-ban aztán a Parlament lehetővé tette, hogy üzletszerzési, közvélemény kutatási vagy tudományos kutatás céljából történő adatkezelések ellen az érintettek tiltakozzanak összhangban az irányelvvel. Ha a tiltakozásnak az adatkezelő nem ad helyt, akkor itt is lehetőség van bírósághoz fordulni.

Az évente egy ingyenes másolathoz való jogot 2009-ben az adatvédelmi biztos viszonylag tágan értelmezte, mert egy banki ügyfél panaszára, aki elveszítette a szerződését az *ingyenes* másolat kiadása mellett foglalt állást. Az erkölcsi bizonyítvány mögött álló, bűnügyi előéleti adatbázisból is kapható ingyenes másolat – azonban ezt nem hatósági erkölcsi bizonyítvány formájában (amely illetékköteles), hanem egy egyszerűbb igazolásként adják ki az érintetteknek. Az egészségügyi adatok másolatáért díjat lehetne felszámítani, azonban az erre vonatkozó rendeletet a miniszter 1997. óta nem készítette el, ezért a felszámított díj jelentősen eltér az egyes szolgáltatóknál. Az adatkezelők a törvényben számukra kötelezően előírt adatkezeléseket az adattovábbítási naplóban nem rögzítik, és mivel más adattovábbítás elvileg kizárt – ez azt is jelenti, hogy sok helyen adattovábbítási napló sincs, még egészségügyi intézményekben sem.

A bírósági érdekérvényesítés folyamata a 17. §-ban van részletezve. Az érintettekre nézve kedvezőtlen, hogy az *adatkezelő székhelye* szerinti bíróságnál lehet keresetet benyújtani. Míg általában polgári perben csak perképes fél ellen lehet pert indítani, addig adatvédelmi ügyekben ilyen korlátozás nincs. A perindítás egyetlen feltétele, hogy az adott entitás legyen az adatkezelő. Ha ez bizonyítható (lásd az adatkezelő definícióját), akkor a per lefolytatható. Jogi személyiség nélküli adatkezelők (szakszervezet, egyház, egyesület, párt, jogi személyiség nélküli cégek, szervezeti egységek, kórházak) ellen is indítható per. A képviselethez ügyvédre sincs szükség, de azért jó, ha van. A bíróság nem a szokásos ügyek között bírálja el a keresetet, hanem *soron kívül*. A per az illetékekről szóló 1990. évi XCIII. törvény 57. § (1) bekezdés o) pontja alapján illetékmentes, a per illeték költséget az állam viseli. A szakértői, illetve ügyvédi költségeket a vesztes félnek meg kell térítenie a nyertesnek. Elvben kérhető a per áthelyezése az érintett lakóhelye szerinti bíróságra is. Országos hatáskörű állami szerv esetén (pl. OEP) a Fővárosi Bíróságnál lehet a pert elindítani. A 18. § szerint az adatkezelők polgári jogi kártérítési felelősséggel is tartoznak, az okozott vagyoni illetve nem vagyoni kárt meg kell téríteniük. Abban vita van a bíróságok ítélkezési

gyakorlatában, hogy az illetékmentesség az ilyen perekre is kiterjed-e. Egyre inkább az a gyakorlat, hogy nem. Az ilyen kártérítési perek után a polgári perrendtartásról szóló 1952. évi III. törvény szerinti illetéket, perköltséget kell fizetni, ami a perelt összeg megadott százaléka, és a vesztes félnek kell állnia.

4.2. A közérdekű adatok nyilvánossága

Az Avtv. 19. §-a előírja az állami-, önkormányzati- vagy közfeladatot ellátó intézmények számára, hogy rendszeresen elektronikusan (vagy más módon) közzé tegyék „*(...) a tevékenységükkel kapcsolatos legfontosabb – így különösen a hatáskörükre, illetékességükre, szervezeti felépítésükre, szakmai tevékenységükre, annak eredményességére is kiterjedő értékelésére, a birtokukban lévő adatfajtákra és a működésükről szóló jogszabályokra, valamint a gazdálkodásukra vonatkozó – adatokat*”. Ha ezek között állam- vagy szolgálati titok, illetve minősített adat van, akkor az a dokumentum nem tehető közzé. A minősített (titkos) iratok minősítésének felülvizsgálatát kezdeményezheti az adatvédelmi biztos (Avtv. 26. § (5) bekezdése), és volt már precedens arra, hogy a biztos felszólalása után a minősítést megszüntették. Bíróságtól is kérhető egyes iratok minősítésének megszüntetése. A TASZ (Társaság a Szabadságjogokért) jogvédő szervezet ezekben a perekben ért már el sikereket. A 19. § (4) bekezdése úgy rendelkezik, hogy a közzé tételre kötelezett szervek, hivatali minőségében eljáró tisztségviselőinek személyes adata közérdekből nyilvános adat, azaz pl. a szerződéseken szereplő aláírásokat és neveket, vagy a határozatot aláíró felelős vezető nevét és hivatali címét is közzé kell tenni. A 19/A. § szerint a minisztériumok döntés előkészítéséhez összegyűjtött adatok tíz évig nem nyilvánosak, bár a megismerésüket korábban is lehetővé lehet tenni. Az elektronikus információszabadságról szóló 2005. évi XC. törvény szerint az államigazgatási szerveknek közzétételi listákat kell készíteniük, amelyen a nyilvánosságra hozni kívánt dokumentumok listája, és a közzé tétel gyakorisága található. A szerv (pl. minisztérium) az alárendeltségébe tartozó intézmények számára ezt a közzétételi listát átadja és a továbbiakban már ez alapján kerül sor mindenhol a közérdekű információk megjelenítésére.

Amennyiben a közérdekű adat nem kerül automatikusan az internetre, úgy bárki kérelmezheti *szóban, írásban vagy elektronikus úton* egy adott intézménytől a számára szükséges közérdekű adatot, dokumentumot. Az adatkezelőnek a legrövidebb idő alatt, de legfeljebb 15 napon belül kell átadni a kért dokumentumot. A törvény jelenleg nem teszi lehetővé azt, hogy az adatkezelőt a közérdekű adat *közzétételére* kötelezze a bíróság, csupán az átadásukat lehet kérni. Az adatkezelő 8 napon belül, megfelelő indoklással megtagadhatja az adatok átadását. Ha a dokumentumokban védendő, nem nyilvános információk vannak, akkor azokat ki kell takarni (felismerhetetlenné kell tenni). A dokumentum kiadásának jogos költségeit az adatkezelő felszámíthatja. Ha a közérdekű adatokhoz a kérelmező nem jut hozzá a megadott időkeretben, akkor 30 napon belül bírósághoz fordulhat és kérheti azt, hogy a bíróság az adatok átadására kötelezze az adatkezelőt. Ugyanúgy, ahogyan a 17. § alapján induló perekben itt is illetékmentességet élveznek a felek, a per illeték költséget az állam viseli. A keresetet a bíróság *soron kívül* bírálja el. Perképességgel nem rendelkező entitás ellen is indulhat per. A 21/A. § szerint a kérelmezőkről személyes adat nem gyűjthető, a dokumentum kiadása után az adatkérő személyes adatait meg kell semmisíteni.

4.3. Az adatvédelmi biztos

Az Avtv. további paragrafusai az adatvédelmi biztos tevékenységével kapcsolatos rendelkezéseket tartalmazzák. A 23. § a biztos megválasztását, a 24. § a biztos tevékenységeit sorolja fel, a 24/A. § a biztos jogállását határozza meg az Országgyűlési biztosokról szóló 1993. évi LIX. törvény paragrafusaihoz viszonyítva. Míg más biztosoknál a személyes érintettség és a jogorvoslati lehetőségek előzetes kimerítése (legalábbis keresése) szükséges eleme egy panasz kivizsgálásának, addig ez az adatvédelmi biztosnál ez nem kötelező. A 25. és a 26. § a biztos intézkedéseit sorolja fel.

Az Adatvédelmi Biztos Hivatala működteti az országos adatvédelmi nyilvántartást is, amelynek a működésére vonatkozó előírások a 28., 29., és 30. §-ban vannak. A nemzeti adatvédelmi nyilvántartásba minden egyes személyes adatot kezelőnek be kell jelentenie a következő adatokat: az adatkezelés célját, az adatok fajtáit és kezelésük jogalapját, az érintettek körét, az adatok forrását, a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, az egyes adatfajták törlési határidejét, az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, valamint a belső adatvédelmi felelős nevét és elérhetőségi adatait. A bejelentés után az adatkezelő egy nyilvántartási számot kap, amelyet később az adatkezelésről adott tájékoztatóban fel kell tüntetnie. A törvény egyes adatkezelőket mentesített a bejelentési kötelezettség alól, pl. ha az adatkezelés munkaviszony, tagsági viszony nyilvántartására szolgál, egyházak belső szabályai szerinti adatkezelés esetén, egészségügyi adatok kezelése esetén, ügyészségi, bírósági adatkezelések esetén stb. A 31. § alapján az adatvédelmi biztos előzetes ellenőrzést tarthat az adatkezelőnél a bejelentés következtében. Erről 8 napon belül értesítést kell küldenie és az ellenőrzést 30 napon belül kell megtartania. Az előzetes ellenőrzés időpontjáig az adatkezelő nem kezdheti meg az adatkezelést. A 31/A. § alapján az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál, pénzügyi szervezeteknél, távközlési és közüzemi szolgáltatóknál belső adatvédelmi felelőst kell kinevezni. A belső adatvédelmi felelős feladatait és kötelességeit a 32. § tartalmazza. Az egészségügyi intézmények is kötelesek belső adatvédelmi felelőst kinevezni az Eüaktv. 32. §-a alapján. Az Avtv. 32. és 32/A. §-a szabályozza azt, hogy statisztikai vagy tudományos kutatás céljából a személyes adatok miképpen kezelhetők.

4.4. Egyéb szektoriális adatvédelmi törvények

A következőkben áttekintünk néhány fontos, személyes adatok kötelező kezelését elrendelő törvényt és néhány hozzájuk kapcsoló Kormányrendeletet, illetve miniszteri rendeletet. Amikor 1991-ben az Alkotmánybíróság meghozta 15/1991. (IV. 13.) számú határozatát az univerzális személyi szám bevezetéséről szóló törvényerejű rendelet ügyében, körvonalazta azt is, hogy minimálisan milyen társadalmi területek szétválasztása lenne indokolt. A határozatban szerepelt, hogy minimálisan az egészségügy, az adóügyek és a népességnyilvántartás területét el kell választani egymástól. Az AB határozat végrehajtása több évet vett igénybe, és végül hosszabb előkészítés után sor került a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény elfogadására. Ez a törvény vezette be az adóazonosító és a társadalombiztosítási azonosító jel (TAJ) fogalmát, szabályozta ezek használatát, a nyilvántartásokat kezelő intéz-

ményrendszert. A korábbi személyi számot is megőrizték mint *személyi azonosító*, de a használatát jelentősen korlátozták. A személyi azonosító a lakcímnyilvántartásban, az ingatlannyilvántartásban, és a választási eljárásban használható. A törvény az azonosító jelek képzését, igénylését és kiadását és megismerhetőségét is szabályozza. Elvben e három terület szétválasztása megtörtént, azonban az állam egyre inkább feszegeti azt a kérdést, hogy egyes esetekben mégiscsak összekapcsolna adatokat a három terület között. Erre az adó-, illeték- és társadalombiztosítási járulék beszedésének esetében, a népszámlálás, valamint a döntéselőkészítéshez szükséges adatok megszerzése ügyében vannak próbálkozások.

Az állampolgárok országos nyilvántartásba vétele Magyarországon az ötvenes években történt meg a személyi igazolvány bevezetéséről szóló 1/1954. (I. 9.) számú Minisztertanácsi rendelet alapján. Ekkor került sor az első személyi igazolványok kiadására. A kezdetben manuális iratkezelést mára már felváltotta egy elektronikus nyilvántartás, amely jelenleg is fejlődik, átalakul. A nyilvántartás a személyi azonosítóval, valamint a természetes azonosítókkal (név, anyja neve, születése hely, idő) határozza meg az állampolgárokat és tárolja lakóhelyüket, tartózkodási helyüket. Ez utóbbiak a régi állandó lakcím, ideiglenes lakcím fogalmaknak felelnek meg. A tartózkodási hely tanuláskor, munkavállaláskor, hosszabb külföldi tartózkodás esetén is biztosítja az állampolgárok (magyar állampolgárok vagy egy EU tagállam polgárainak) elérhetőségét. Ennek az adatbázisnak a működését szabályozza a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény. Az okmányirodák tevékenységét, a bejelentések módjának részletszabályait pedig a hozzá kapcsolódó, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról szóló 146/1993. (X. 26.) Kormányrendelet. Az újszülött állampolgárok születésük után, a kórház bejelentése és az anya (valamint az apa) nyilatkozata alapján kapják meg a személyi számukat, nevüket, és kerülnek be az országos nyilvántartásba az anya lakcímével. Miután a rekordjuk létrejött, akkor ennek másolataként születési anyakönyvi kivonatot és lakcímkártyát kapnak. Ha a szülők kívánják, személyi igazolványt és/vagy útlevelet is kérhetnek az újszülöttnek.

Az állampolgárok lakcímnyilvántartásából magán- és jogi személyek (pártok, egyesületek, vállalatok) címlistákat kérhetnek le, alapvetően reklám, marketing, üzletszerzés céljából, illetve a pártok a választóikkal történő kapcsolatfelvétel céljából. E célok érdekében kizárólag csoportos lekérést lehet végrehajtani. Egy-egy konkrét személy lakcímének megszerzésére akkor van mód, ha valaki a jegyzőnél igazolja, hogy jogos érdeke fűződik ahhoz, hogy egy adott személy lakcímét megtudja. A bírósági perindítás, rendőrségi nyomozás, baleset utáni tanú kutatás ilyen jogos érdek. A lakcímnyilvántartásból történő adatkérésnek díja van, amelyet a polgárok személyi adatainak és lakcímének nyilvántartásából teljesített adatszolgáltatásért, a kapcsolatfelvétel céljából való megkeresésért, valamint értesítésért fizetendő igazgatási szolgáltatási díjról szóló 16/2007. (III. 13.) IRM-MeHVM együttes rendelet szabályoz. Ebből a jogszabályból megtudhatjuk, hogy hol, hogyan jelenthetjük be ilyen listákra az igényünket. A listákat elektronikus adathordozón vagy öntapadós etiketteken is tudják biztosítani. Az állampolgárok a személyes lakcím adataiknak üzletszerzési célból történő felhasználását megtilthatják. Ehhez be kell fáradniuk egy okmányirodába vagy igénybe vehetik a Magyarorszag.hu Kormányzati Portál szolgáltatásait is. Egy adatlap kitöltésével felkerülhetnek az ún. Robinson-listára. Céges megkeresésekkor nem fog megjelenni a lakcímük az átadásra kerülő adatok között.

A Magyar Köztársaság az állampolgárok számára elektronikus Kormányzati Portált, ügyfélkaput és több hasznos szolgáltatást üzemeltet az interneten, amelyet a következő

címen érhetnek el: http://www.magyarorszag.hu. Okmányirodai regisztráció után a felhasználók hozzáférési azonosítót és jelszót kapnak az elektronikus szolgáltatásokhoz. Ezek között, elektronikus adóbevallás, okmányirodai ügyintézés elindítása, időpontfoglalások, TAJ alapú szolgáltatások, számos hivatalos űrlap, központi értesítési tárhely, és még sok hasznos szolgáltatás kapott helyet. A portál működését az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény szabályozza. Az állampolgárok számára biztosítandó egyes közérdekű adatok nyilvánosságra hozását, a jogalkotás nyilvánosságát az elektronikus információszabadságról szóló 2005. évi XC. törvény szabályozza. Ebben a törvényben találjuk a Magyar Köztársaság hivatalos lapjának a Magyar Közlönynek az ingyenes és elektronikus közzé tételéről szóló paragrafusokat, valamint ez a törvény kötelezi a minisztériumokat, hivatalokat, önkormányzatokat, közfeladatot ellátó szervezeteket hogy a kezelésükben található egyes közérdekű adatokat az interneten közzé tegyék.

Az állam bűnmegelőzési és bűnüldözési célból rendőrséget tart fent. Ez a szervezet számos erős jogosítványt kapott feladata végrehajtásához. Az adatvédelmi jog a bűnüldözés, bűnmegelőzés célját kivételesnek tekinti és ebben a körben különböző kényszerintézkedéseknek van helye. A rendőrség gyakorlatilag minden számára szükséges személyes adathoz hozzájuthat, közöttük különleges személyes adatokhoz. A rendőrség titkos megfigyelési módszerekkel, házkutatással, motozással is élhet. A rendőrség adatkezelését, a Rendőrségről szóló 1994. évi XXXIV. törvény szabályozza. A később ártatlannak bizonyult személyek adatait meg kell semmisítenie. A törvény szabályozza azt is, hogy a rendőrség milyen állami szervektől igényelhet adatokat, hová kell, hogy forduljon az adatokért, és a gyűjtött adatokat milyen őrzési idő után kell megsemmisíteni. A Parlament törvényben szabályozta a magánnyomozók és vagyonőrök adatkezelését. Ezek a szabályok a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényben találhatók.

Az országos közlekedési nyilvántartásban a Magyarországon regisztrált gépjárművek, a kiadott vezetői és (mozgássérült) parkolási engedélyek adatai találhatók meg. A gépjárművek egységes nyilvántartásban szerepelnek, amely rendszám (hatósági jelzés) és más azonosító adatok (alváz-, motor-, és gyári szám, típus, szín) alapján azonosítja a gépjárműveket. Ez az adatbázis a gépjárművek tulajdonosainak, illetve üzemben tartóinak közhiteles adatait is tartalmazza, így könnyen megállapítható egy ellopott, balesetet szenvedett jármű tulajdonosának a kiléte. Alkalmas arra is, hogy a gépjárművel kapcsolatos adó-, illetve illeték fizetési kötelezettség teljesítését ellenőrizni lehessen. A vezetői engedélyek nyilvántartása, érvényessége, visszavonása, a parkolási engedélyek érvényessége, visszavonása ugyancsak szerepel az adatbázisban. A nyilvántartás működtetése az okmányirodákon keresztül történik. Itt kell bejelenteni a gépjárművekhez kapcsolódóan a tulajdonosváltást, forgalomba helyezést, forgalomból kivonást és megfizetni az ezzel kapcsolatos illetékeket; itt tartják nyilván a jogosítványszerzést, érvényesítést, elvesztést, bevonást. Van mód az adatbázisból csoportos adatkérésekre, amely adatokat üzletszerzésre, reklámcélokra, vagy tudományos kutatásra lehet használni. A közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény tartalmazza a nyilvántartás működésére vonatkozó szabályokat.

A magyar törvények szerint minden gépjárműre kötelező felelősség biztosítást kell kötni. A kötelező felelősség biztosítás ellenőrzésére, a károk megtérítésének felgyorsítására hozta létre a magyar állam 2009-ben a biztosítási Információs Központot. Ebben a biztosítók bejelentése alapján nyilvántartják, hogy mely gépjárművet a tulajdonosa mely biztosító társaságnál biztosította, továbbá nyilvántartják a gépjármű kártörténeti eseményeit, a tulajdonos (szerződő) személyi adatait. Ennek az adatbázisnak alapvetően az a célja, hogy ki-

szűrje azokat a gépjárműveket, amelyeket nem biztosítottak. A jogszabályok alapján, az ilyen gépjárműveket ki lehet vonni a forgalomból. A központi kártörténeti lista pedig egyszerűvé és követhetővé teszi az egyes tulajdonosok bonus/malus besorolását, amely alapján a biztosítók az ajánlatukat megteszik. Az Információs Központra vonatkozó adatvédelmi szabályok a kötelező gépjármű-felelősségbiztosításról szóló 2009. évi LXII. törvényben találhatók.

Az országban a telkek és házak, lakások tulajdonjogai egy országos ingatlan-nyilvántartó rendszerben találhatók. Az ingatlan-nyilvántartásról szóló 1997. évi CXLI. törvény szabályozza az adatbázis működését, amely kezdetben papír alapú volt és a földhivatalok kezelték, azonban ma már országos, GPS műholdtérkép és koordináta alapú országos nyilvántartássá nőtte ki magát. A bejegyzéseket kérelemre, megfelelő, ügyvéddel ellenjegyzett, hitelesített eredeti okmányok csatolása esetén végzi el a földhivatal. Az ingatlanok státusza a Ptk. alapján meglehetősen bonyolult lehet. A résztulajdon, szolgalmi jog, használati jog, elővásárlási jog, öröklés, tulajdonmegosztás, jelzálog, bírósági ítéletek végrehajtása bonyolíthatja egy-egy ingatlan jogi helyzetét. Egy ingatlan adatait az ún. tulajdoni lap tartalmazza, amelyen minden korlátozás és feljegyzés, megjegyzés, korlátozás szerepel. A nyilvántartás alapvetően nyilvános, ezért ki-ki megismerheti egy telek vagy lakás tulajdonviszonyait és ennek ismeretében dönthet a megvásárlásáról. A tulajdonos pontos azonosítására a személyi azonosítót (korábban személyi szám) és a természetes azonosító adatokat használják.

Az államigazgatás megköveteli a társadalmi élettel kapcsolatos statisztikai adatok gyűjtését. A KSH[33] (Központi Statisztikai Hivatal) feladata az adatbejelentésre kötelezettektől érkező táblázatok és adatok összesítése és megfelelő prezentációja. Az országos adatgyűjtést a statisztikáról szóló 1993. évi XLVI. törvény szabályozza. A személyes adatok használatát ez a törvény általában tiltja, mert nincs rá szükség. Személyes adatokat statisztikai célra az érintett hozzájárulásával lehet kezelni, vagy ha ezt egy törvény kötelezően elrendeli. A statisztikáról szóló törvényt minden évben egy Kormányrendelet egészíti ki, amely a következő évre érvényes OSAP (Országos Statisztikai Adatgyűjtési Program) táblázatait és a jelentések gyakoriságát tartalmazza. A legutóbbi Kormányrendelet az Országos Statisztikai Adatgyűjtési Program adatgyűjtéseiről és adatátvételeiről szóló 288/2009. (XII. 15.) Kormányrendelet. A KSH demográfiai statisztikát is vezet, a népesség nyilvántartó hivataltól kapott adatok alapján a születések számára, a családokban nevelt gyerekek számára, a házasságkötésekre, és a halálozások számára és a halálokokra vonatkozóan. Ezek az adatok összesítve a KSH honlapján is megtekinthetők.

A személyes adatokat kezelő szolgáltatóktól, intézményektől tudományos kutatás, közvélemény kutatás vagy üzletszerzés céljából címlistákat lehet kérni. Ebben csak a név és a levelezési cím szerepelhet. A címlista biztosítja azt a lehetőséget, hogy a kutató felvegye az érintettekkel a kapcsolatot és tőlük további adatokat, véleményeket kérjen, vagy számukra reklámanyagokat postázzon. Az Avtv. 16/A. §-a előírja azt, hogy ebben az esetben az érintettek tiltakozási jogát biztosítani kell. Ez úgy történik, hogy az adatkezelés előtti tájékoztatás során fel kell vetni ezt a lehetőséget és kérni az érintettek hozzájárulását egy ilyen adatkezeléshez. Az erre vonatkozó eljárásrendet a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény tartalmazza.

[33] Honlapja: http://www.ksh.hu

A titkos iratokat nem, de a minősített adat védelméről szóló 2009. évi CLV. törvény szövegét minden magyar állampolgár megismerheti. Ez a frissen megalkotott törvény radikálisan új megoldásokat alkalmaz a korlátozott terjesztésű, bizalmas, titkos, és a szigorúan titkos dokumentumok kezelésére. A korábbi törvény lehetővé tette, hogy egy titokköri jegyzék alapján a tartalomtól függetlenül, automatikusan titkossá minősítsenek dokumentumokat, aminek köszönhetően temérdek minősített irat keletkezett. Az új rendszerben a tartalom alapján, szigorú kritériumok alapján lehet csak valamit minősíteni, amit rendszeresen felül kell vizsgálni. A törvény létrehozta a Nemzeti Biztonsági Felügyeletet, amely szervezet felügyeli a minősített iratokat kezelő szervezetek tevékenységét, és számukra biztonsági és szervezési szolgáltatásokat nyújt. A felügyelet szervezi meg a rejtjelezést, végzi az elektronikus rendszerek biztonsági engedélyezését, ellenőrzi az adatkezelési folyamat biztonságosságát, a minősítési folyamat megfelelőségét stb.

A rendszerváltás után a korábbi szocialista hatalom által gyűjtött adatokat nem semmisítették meg, hanem egy részüket egy levéltárban gyűjtötték össze. A levéltárba történő adattovábbítás, adatátadás rendjét, valamint az ott folyó kutatás módját az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról szóló 2003. évi III. törvény írja le. A törvényt számos kritika érte. Egyrészt, mert nem tudta elérni, hogy minden fontos irat a levéltárba bekerüljön. Sokat még mindig a Belügyminisztérium őriz. Másrészt, az iratok kiadását akadályozhatja a levéltár vezetése. A kiadott iratokat anonimizálni kell, ami azt jelenti, hogy minden nevet, dátumot és helyszínt törölnek. Különleges személyes adatokat eleve nem adnak ki, ezért a hölgy/úr ismerősök nevét sem lehet megismerni. Továbbá a levéltári anyagokban szereplő érintettek 90 évre megtilthatják a személyes adataik felhasználását. Ezek nehezítik a történelmi igazság kiderítését. Azok számára, akik szenvedői voltak a múlt rendszernek – megfelelő szintű adatvédelmet biztosít a törvény, a történészeknek inkább az fáj, hogy a rendszer irányítóinak tevékenységét is egyazon módon nehezíti meg.

A Magyar Köztársaságban a fenti speciális levéltáron kívül több közlevéltár is található, amelyek leginkább történeti kutatások végzésére szolgálnak. A levéltárban elhelyezett dokumentumok természetesen sok személyes adatot tartalmaznak. Az érintettek érdekeit az védi, hogy a dokumentumokat csak haláluk vélelmezett időpontja után lehet kutatni, addig pedig csak anonimizált formában lehet tanulmányozni azokat. A közlevéltárakban alapvetően kutatók, kutatási engedély alapján dolgoznak. Megbízás alapján természetesen egyedi dokumentumokat is felkutatnak, pl. családfakutatás, tulajdonlás, iskolai végzettség és egyéb ügyekben. A nem állami kezelésben lévő levéltárak (alapvetően az egyházi levéltárak) működését is törvény szabályozza, mint ahogyan a magánszemélyek tulajdonában lévő értékesíteni szándékozott régi iratok megszerzését, védetté nyilvánítását. A törvény nem tesz különbséget az általános levéltárak és az egészségügyi dokumentumokat tároló Semmelweis Orvostörténeti Levéltár működése között. Ez jelentős probléma, mert ez utóbbi *szaklevéltárban* különleges személyes adatokat őriznek, amelyek gyűjtése az érintettek hozzájárulása nélkül történik ma is. A levéltárak működését a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény szabályozza. A törvény alkalmazását elősegítendő és részletes szabályozást tartalmazó Kormányrendelet jelent meg 2005-ben: a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Kormányrendelet.

Az itt felsorolt törvényeken kívül még számos törvény tartalmaz személyes adatok kezelését szabályozó rendelkezéseket. A magyarorszag.hu oldalon végzett keresés alapján 2010-ben a személyes adat szókapcsolat összesen 765 jogszabályban szerepel, amelyből

317 a Parlament által elfogadott magyar törvény, a fennmaradó 448 pedig Kormányrendelet vagy rendelet.

Ellenőrző kérdések

1. Az Alkotmány mely szakaszai kapcsolódnak a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához?

2. Milyen fontos definíciót tartalmaz az Alkotmánybíróság 15/1991. számú határozata és ismertesse e definíció lényeges elemeit?

3. Mely törvény szabályozza a Magyar Köztársaságban a személyes adatok védelmét?

4. Mely adatkezelőkre vonatkozik a magyar adatvédelmi törvény?

5. A magyar adatvédelmi törvény szerint mikor lehet személyes adatokat kezelni?

6. Vonatkozik-e az adatvédelmi törvény a személyes levelező programokban található címtárra?

7. Mit jelent az életfontosságú érdekből történő adatkezelés?

8. Mit foglal magában az adatvédelmi tájékoztatás?

9. A magyar érintettek milyen jogait tartalmazza az adatvédelmi törvény?

10. Milyen jogorvoslati lehetőséggel élhet az, akinek valamilyen adatvédelemhez kapcsolódó jogát egy adatkezelő nem biztosította, megsértette?

11. Mely adatok tekinthetők közérdekű adatnak?

12. Mit jelent a közérdekből nyilvános adat fogalom?

13. Milyen lehetőségek vannak egy titkossá minősített irat titkosságának feloldására?

14. Soroljon fel néhány szolgáltatást, amelyet az elektronikus Kormányzati Portál biztosít?

15. Milyen nagy országos adatbázisokat ismer? Mely törvények szabályozzák ezekben az adatok kezelését?

5. Az egészségügyi adatok kezelésével kapcsolatos jogszabályok

Az Európai Unió területén a különleges személyes adatok kezelése általában tilos. Az Európai Parlament 95/46/EK adatvédelmi irányelve két kivételt enged meg: a bűnügyi személyes adatok kezelését egy erre kijelölt hatóság számára, valamint személyes egészségügyi adatok kezelését egy erre kijelölt, szakmai titoktartásra kötelezett egészségügyi ellátó szervezet dolgozói számára. A bűnügyi személyes adatok kezelésében Magyarországon a közelmúltban jelentős változások történtek, ugyanis az Alkotmánybíróság a Köztársasági Elnök Hivatalának indítványára több egymásnak ellentmondó rendeletet, Kormányrendelet részletet, törvényi paragrafusokat semmisített meg. Az indítvány közvetlen előzménye az USA és Magyarország között kötendő bűnmegelőzési, bűnüldözési nemzetközi egyezmény megkötése volt a kölcsönös vízummentesség megteremtése érdekében. Ekkor derült fény számos anomáliára az adatkezeléseket szabályozó rendszerben, amelyeket sürgősen orvosolni kellett.[34] A bűnügyi nyilvántartás több esetben nem különböztette meg a tanukat, a sértetteket, a gyanúsítottakat, és az elítélteket egymástól. A szabályozás sok esetben rendeleti szinten történt, máskor nem volt szabályozva az adatmegőrzés ideje. Ugyanakkor fontos megjegyezni, hogy a korábban ismertetett EJEE egyezmény, és az EU 95/46/EK adatvédelmi irányelve is lehetővé teszi, hogy bűnügyi személyes adatokat egy törvény előírása alapján kényszerintézkedés részeként, kötelező módon lehessen kezelni. Ilyen esetekben az érintettek adatvédelemhez fűződő jogait korlátozni is lehet. A jegyzet ezzel a területtel részletesen nem foglalkozik részletesebben. Az érdeklődők részletes beszámolót olvashatnak erről Dr. Jóri András, Dr. Hegedűs Bulcsú és Dr. Kerekes Zsuzsanna szerkesztésében megjelent Adatvédelem és információszabadság a gyakorlatban c. könyvben.

A továbbiakban az emberi jogok szempontjából érdekesebb, az emberi méltóságot komolyan érintő, egészségügyi adatok kezelését tekintjük át. A már megismert EU dokumentumokon kívül, az Európa Tanács 1997-ben tető alá hozott egy ajánlást, amely több európai uniós egyezmény és más dokumentum figyelembe vételével készült, és amely az egészségügyi adatok védelmének alapvető követelményeit foglalta össze a tagállamok számára.[35] Az R(97) No. 5. számú ajánlást a korábbi 1981-es adatvédelmi ajánlás helyett hozták létre a technikai fejlődés következtében fellépő új problémák és a személyes genetikai adatok megjelenése miatt. Az ajánlás betartására a Magyar Köztársaság írásban kötelezettséget vállalt. Az ajánlás 4. cikke fontos alapvetéseket tesz az egészségügyi adatok kezelése tekintetében:

> 4. Orvosi adatok gyűjtése és feldolgozása
>
> 4.1. Orvosi adatokat tisztességesen és törvényesen kell gyűjteni és feldolgozni és csak meghatározott célból.
>
> 4.2. Orvosi adatot alapvetően az érintett személytől kell beszerezni. Más forrásból csak akkor szerezhetők be, ha ez összhangban áll ennek az ajánlásnak a 4., 6., és 7.

[34] Az Alkotmánybíróság eljárásáról Dr. Kadlót Erzsébet tartott előadást az Adatvédelmi Biztos Hivatala rendezésében tartott World Wide Identity 2009 konferencián. A fóliák elérhetők az adatvédelmi biztos honlapjáról.

[35] Az Európa Tanács és a Miniszterek Tanácsának az egészségügyi adatok védelmével kapcsolatos R (97) 5 (1997. február 13.) számú ajánlása, elérhető az Európa Tanács honlapján.

pontjával, és ha ez szükséges a feldolgozás céljának eléréséhez, vagy ha az érintett nincs abban a helyzetben, hogy az adatokat megadhassa.

4.3. Orvosi adatokat akkor lehet gyűjteni és feldolgozni, ha:

a) a törvény kötelezően előírja:

i) közegészségügyi okokból; vagy

ii) a 4.8 pont figyelembe vételével, valódi veszélyhelyzet elkerülése vagy egy bizonyos bűncselekmény megakadályozása érdekében; vagy

iii) más fontos közérdekből; vagy

b) a törvény megengedi:

i) megelőző orvoslás céljából, diagnosztikai vagy terápiás célokból az érintett személyre vagy genetikai vonalában előforduló rokonára vonatkozóan; vagy

ii) az érintett vagy egy harmadik személy életfontosságú érdekének megvédése céljából; vagy

iii) adott szerződéses kötelezettség teljesítése érdekében; vagy

iv) jogi követelés megalapozása, érvényesítése vagy megvédése érdekében; vagy

c) ha az érintett személy vagy törvényes képviselője vagy egy hatóság vagy bármely személy vagy testület, amelyet a törvény erre kijelöl egy vagy több cél érdekében a beleegyezését adta, amennyiben a nemzeti törvény nem rendelkezik másként.

Az ajánlás három alapvető esetet különböztetett meg az adatkezelésre vonatkozóan: amikor egy törvény az egészségügyi adatok kezelését elrendeli (közegészségügyi okból, bűnmegelőzési okból, vagy egyéb fontos közérdekből); amikor az adatok kezelését a törvény megengedi (normál orvosi ellátás céljából, életfontosságú érdekből, szerződéses kötelezettség teljesítése érdekében, jogi követelés alátámasztása érdekében), illetve más esetekben, amikor az érintett vagy törvényes képviselője az adatkezeléshez hozzájárul. Természetesen a kötelezően elrendelt adatkezelés egyfajta kényszerintézkedés, amely esetben az adatvédelemhez kapcsoló jogokat egy törvénnyel korlátozni lehet. Amikor az adatkezelést a törvény *megengedi*, akkor az érintettek jogait az adatkezelő alapvetően nem korlátozhatja. Az érintett tiltakozhat az adatkezelés ellen, és bírósághoz is fordulhat, ha úgy érzi valamilyen jogát megsértették.

Az R(97) No. 5. ajánlás lehetővé teszi azt, hogy egészségügyi adatokat töröljenek:

10.1. Általában az orvosi adatokat nem lehet tovább tárolni, mint amely szükséges annak a célnak az eléréséhez, amelynek érdekében az adatokat gyűjtötték és feldolgozták.

10.2. Amikor a közegészség, az orvostudomány törvényes érdekében – vagy, hogy az orvosi kezelésért felelős személy vagy az adatállomány kezelője számára lehetővé váljon egy jogi igény védelmezése vagy érvényesítése – vagy történelmi vagy statisztikai okokból szükségesnek bizonyul az orvosi adatok további tárolása, amely a továbbiakban már nem az eredeti célokra szolgál, megfelelő technikai intézkedéseket kell tenni az adatok korrekt megőrzése és biztonsága érdekében figyelembe véve a páciensek magánéletének védelmét.

> 10.3. Az érintett kérésére az orvosi adatait törölni kell – kivéve, ha azokat már anonimizálták vagy van elsőbbrendű törvényes érdek, elsősorban a 10.2 pontban felsoroltak, arra, hogy ezt ne tegyék, vagy ha az adatok nyilvántartása kötelezettség.

Az egészségügyi adatok kutatási célú felhasználását alapvetően akkor teszi lehetővé, ha erről a lehetőségről az érintettet előzetesen tájékoztatják és az nem emelt kifogást ez ellen.

5.1. Az Alkotmánybíróság néhány egészségügyi határozata

A továbbiakban néhány, az egészségügyi önrendelkezés témájába vágó alkotmánybírósági határozat kerül bemutatásra.

Az AB egy indítvány nyomán vizsgálta a személyes egészségügyi adatok definícióját. A 65/2002. (XII. 3.) számú határozat szerint alkotmányellenes az Eüaktv.-ben szereplő definíció, amely szerint a szexuális szokásokra vonatkozó személyes adatok beletartozhatnak az egészségügyi adatok fogalmába. Az indítványozó szerint azzal, hogy az Eüaktv. számos esetben törvényi kényszerrel rendeli el ilyen adatok továbbítását (bennük a szexuális szokásokra vonatkozó adatokét) jelentősen sérti az állampolgárok magánéletének tiszteletben tartására vonatkozó jogot. Az AB az indítványnak helyt adott. Ugyanakkor az ítélet jóval több problémát generált, mint amennyit megoldott. Az ítéletet a mai napig nem tartja tiszteletben a társadalombiztosítás, mivel számos szexuális szokásra utaló személyes adatot kezel.

> (…) a jogalkotó **a személyes adatok, illetve a szigorúbban védett különleges adatok kezelését akkor rendelheti el, „ha az adatkezelés lehetővé tételével egyidejűleg meghatározza az adatkezelés pontos feltételeit, azaz az Alkotmány 59. § (1) bekezdésben garantált személyes adatokhoz való alapjog korlátozásának konkrét részletszabályait.**” (ABH 2002, 357, 363.)

Az Alkotmánybíróság indítvány nyomán vizsgálta a védőoltások megtagadásakor fellépő helyzetben a jogorvoslat lehetőségét. A kérelmező hosszú évek óta próbálta elérni, hogy amikor *kötelező jellegű* védőoltás alkalmazására kerül sor, akkor az egészségügyi rendszer erre szólítsa fel a kötelezettet és biztosítsa az Alkotmány 57. §-ában biztosított fellebbezés lehetőségét. A probléma folyamatosan jelen van az egészségügyben, és még ma is többször előfordul, hogy hatósági egészségügyi eljárásra kerül sor, annak jogi háttere nélkül. A 39/2007. (VI. 20.) AB határozat helyt adott az indítványtevő 1996-ban benyújtott indítványának.

> (…) Az Alkotmánybíróság – hivatalból eljárva – megállapítja: az Alkotmány 50. § (2) bekezdését és az 57. § (5) bekezdését sértő, mulasztásban megnyilvánuló alkotmányellenes helyzet jött létre annak következtében, hogy **az Országgyűlés nem biztosított hatékony jogorvoslati eszközt a kötelező védőoltás alóli mentesítés megtagadásával szemben.** Az Alkotmánybíróság felhívja az Országgyűlést, hogy jogalkotási feladatának 2008. március 31-ig tegyen eleget.

Az Alkotmánybíróság egy indítvány alapján vizsgálta az orvosi receptek adattartalmát szabályozó rendeleteket. A szabályozást alkotmányellenesnek találta és egyes paragrafuso-

kat megsemmisített. Ezek szerint az olyan orvosi recepteken, amelyek támogatás nélkül rendelnek gyógyszert, alkotmányellenes a TAJ és a BNO feltüntetése. Az AB a 29/2009. (III. 20.) számú határozatában leszögezte:

> (…) Az Eüaktv. jelenleg is htályos 4. § (2) bekezdés g) pontja értelmében egészségügyi és személyazonosító adatot a 4. § (1) bekezdésében foglaltakon túl — törvényben meghatározott esetekben — az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának, valamint a gazdaságos gyógyszer-, gyógyászati segédeszköz- és gyógyászati ellátás rendelési szabályai betartásának a vizsgálata, továbbá a külön jogszabály szerinti szerződés alapján a jogosultak részére nyújtott ellátások finanszírozása, illetve az ártámogatás elszámolása céljából lehet kezelni. Az Eüaktv. 22. §(1) bekezdés c) pontja úgy rendelkezik, hogy **a társadalombiztosítási igazgatási szervek részére abban az esetben továbbítható egészségügyi és személyazonosító adat, amennyiben az a 4. § (2) bekezdés g) pontjában foglalt célok teljesítéséhez szükséges.** A 22. § (2) bekezdése értelmében az egészségügyi és személyazonosító adatokat a társadalombiztosítási igazgatási szervek kizárólag az ellátás megállapításával, folyósításával, az ellenőrzés lefolytatásával, egészségbiztosítási orvosszakértői, illetve jogorvoslati tevékenységgel megbízott dolgozója, továbbá a 4. § (2) bekezdés g) pontja szerinti feladat teljesítésével megbízott munkatársa kezelheti. (…)
>
> (…) Az Ebtv. [A kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény] kiegészült a 79/A. §-sal, melynek (1)-(2) bekezdése értelmében az egészségbiztosító az Ebtv. alapján kötött szerződésekhez kapcsolódóan az Eüak. 4. § (2) bekezdés g) pontjában foglalt célok teljesítése érdekében kezeli az Eüak. 22. §-ának (5) bekezdésében meghatározott adatokat. Az egészségügyi szolgáltató ezen adatok kezelését, az egészségbiztosító felé történő továbbítását a külön jogszabályban és a szerződésében előírt formában és módon teljesíti.
> A fentiekből megállapíthatóan **az Ebtv. és az Eüaktv. idézett előírásaiból fakad az, hogy a társadalombiztosítási igazgatási szerv, nevezetesen az egészségbiztosító az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának vizsgálata, illetve a jogosultak részére nyújtott ellátások finanszírozása céljából kezelheti az Eüaktv. 22. § (5) bekezdésében foglalt adatokat.** E célok érdekében az egészségügyi szolgáltató köteles a megjelölt adatokat az egészségbiztosító felé továbbítani.

5.2. Az egészségügyi adatok védelméről szóló törvény

A Magyar Köztársaság állami egészségügyi ellátó hálózatot és ehhez ugyancsak állami egészségbiztosítót működtet. Az egészségügyi rendszernek nemcsak gyógyítási, hanem egészség megőrzési, megelőzési, hatósági ellenőrzési jogai is vannak. Az egészségügyi rendszerben számos adatkezelő végez kiterjedt adatkezelést. Ezért a Parlament egy külön szektoriális adatvédelmi törvényt alkotott, amely a személyes egészségügyi adatok kezelését szabályozza. Ennek a neve: az egészségügyi és a hozzájuk tartozó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, röviden: Eüaktv. Az Avtv. 3. § (2) bekezdésének előírása szerint, különleges személyes adat mikor kezelhető, azt egy tör-

vény kötelezően elrendeli (ez az Eüaktv.), vagy az érintett írásban beleegyezik. Az egészségügyi adatkezelés alapja egy törvényi kötelezettség.

Az Eüaktv. 2. §-a kiterjeszti a törvény hatályát minden egészségügyi ellátást nyújtó szervezetre és személyre tehát minden adatkezelőre, illetve minden olyan személyre, aki az ellátásokat igénybe veszi függetlenül attól, hogy beteg-e vagy egészséges. A 3. § a törvényben alkalmazott definíciókat sorolja fel, míg a 4. §-a határozza meg azokat a törvényes célokat, amelyek érdekében egészségügyi adat kezelhető. Emlékezzünk vissza arra, hogy az Avtv. előírása szerint személyes adat csak törvényes célból kezelhető. Ezek a célok láthatók az alábbiakban.

> 4. § (1) Az egészségügyi és személyazonosító adat kezelésének célja:
>
> a) az egészség megőrzésének, javításának, fenntartásának előmozdítása,
>
> b) a betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is,
>
> c) az érintett egészségi állapotának nyomon követése,
>
> d) a népegészségügyi [16. §], közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
>
> e) a betegjogok érvényesítése.
>
> (2) Egészségügyi és személyazonosító adatot az (1) bekezdésben meghatározottakon túl – törvényben meghatározott esetekben – az alábbi célból lehet kezelni:
>
> a) egészségügyi szakember-képzés,
>
> b) orvos-szakmai és epidemiológiai vizsgálat, elemzés, az egészségügyi ellátás tervezése, szervezése, költségek tervezése,
>
> c) statisztikai vizsgálat,
>
> d) hatásvizsgálati célú anonimizálás és tudományos kutatás,
>
> e) az egészségügyi adatot kezelő szerv vagy személy hatósági vagy törvényességi ellenőrzését, szakmai vagy törvényességi felügyeletét végző szervezetek munkájának elősegítése, ha az ellenőrzés célja más módon nem érhető el, valamint az egészségügyi ellátásokat finanszírozó szervezetek feladatainak ellátása,
>
> f) a társadalombiztosítási, illetve szociális ellátások megállapítása, amennyiben az az egészségi állapot alapján történik,
>
> g) az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának, valamint a gazdaságos gyógyszer-, gyógyászati segédeszköz- és gyógyászati ellátás rendelési szabályai betartásának a vizsgálata, továbbá a külön jogszabály szerinti szerződés alapján a jogosultak részére nyújtott ellátások finanszírozása, illetve az ártámogatás elszámolása,
>
> h) bűnüldözés, továbbá a rendőrségről szóló 1994. évi XXXIV. törvényben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés,
>
> i) a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása, az abban kapott felhatalmazás körében,

j) közigazgatási hatósági eljárás,

k) szabálysértési eljárás,

l) ügyészségi eljárás,

m) bírósági eljárás,

n) az érintettnek nem egészségügyi intézményben történő elhelyezése, gondozása,

o) a munkavégzésre való alkalmasság megállapítása függetlenül attól, hogy ezen tevékenység munkaviszony, közalkalmazotti és közszolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik,

p) közoktatás, felsőoktatás és szakképzés céljából az oktatásra, illetve képzésre való alkalmasság megállapítása,

q) a katonai szolgálatra, illetve a személyes honvédelmi kötelezettség teljesítésére való alkalmasság megállapítása,

r) munkanélküli ellátás, foglalkoztatás elősegítése, valamint az ezzel összefüggő ellenőrzés,

s) az egészségügyi ellátásokra jogosultak részére vényen rendelt gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás folyamatos és biztonságos kiszolgáltatása, illetve nyújtása érdekében,

t) a munkabalesetek, foglalkozási megbetegedések – ideértve a fokozott expozíciós eseteket is – kivizsgálása, nyilvántartása és a szükséges munkavédelmi intézkedések megtétele.

(3) Az (1)-(2) bekezdésekben meghatározott céloktól eltérő célra is lehet az érintett, illetve törvényes vagy meghatalmazott képviselője (a továbbiakban együtt: törvényes képviselő) – megfelelő tájékoztatáson alapuló – írásbeli hozzájárulásával egészségügyi és személyazonosító adatot kezelni.

(4) Az (1)-(2) bekezdések szerinti adatkezelési célokra csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges.

Az 5. § a lehetséges adatkezelőket sorolja fel. A 7. § az érintettek jogait tartalmazza, amelyek közül megemlíthető a titoktartáshoz való jog, a másolatkérés, a betekintés joga, illetve egy összefoglaló biztosítása, amelyben az érintettet tájékoztatják aktuális egészségi állapotáról. Az elhunytak házastársai, egyenesági leszármazottai hozzájuthatnak bizonyos egészségügyi adatokhoz, amelyek a halál közvetlen okára vonatkoznak, illetve ha a közeli hozzátartozók gyógykezeléséhez elengedhetetlenül fontos adat más módon nem szerezhető meg. A 10. § a különböző szolgáltatóknál rendelkezésre álló adatok összekapcsolását szabályozza. E szerint az adatok összekapcsolása csak akkor végezhető el, ha ezt az érintett nem tiltja meg, és ennek a lehetőségéről tájékoztatni kell. Sürgős életveszélyes helyzetben azonban az adatok beleegyezés nélkül is összekapcsolhatók. Egy offline rendszerben az ilyen szabályozás tud működni, mert a páciens tud alapvetően tájékoztatást adni arról, hogy egyáltalán mely más intézményben vannak meg az adatok. Egy online intézményközi rendszerben azonban az adatok azonnal lekérhetők a páciens adatainak megadásával bármely, a rendszerben lévő szerverről. Az online rendszer jogi szabályozása egyelőre még várat magára. 2008 és 2009 között egy évig hiányzott a 10. § (1), (2) és (3) bekezdése, mi-

vel egy pilot intézményközi rendszert épített az Egészségügyi Minisztérium, amelyben a páciensek adatait beleegyezésük nélkül kapcsolta össze. Azért hogy ez ne legyen törvényellenes, törölték az itt megadott három bekezdést. 2009. január 1-jétől azonban visszaállították az eredeti állapotot.

> 10. § (1) A 4. § (1)-(3) bekezdése szerinti célból történő adatkezelés és adatfeldolgozás esetén az egészségügyi ellátóhálózaton belül az egészségügyi és személyazonosító adatok továbbíthatók, illetve összekapcsolhatók. Az egészségbiztosítási szervnek a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény (a továbbiakban: Ebtv.) 81. §-ában meghatározott feladata ellátása érdekében egészségügyi adatok és TAJ-számok az egészségügyi ellátóhálózat és az egészségbiztosítási szerv között is továbbíthatók és összekapcsolhatók, a feladat ellátásához szükséges mértékben. A különböző forrásból származó egészségügyi és személyazonosító adatokat csak addig az időpontig és olyan mértékig lehet összekapcsolni, ameddig az a megelőzés, a gyógykezelés, a népegészségügyi, közegészségügyi-járványügyi intézkedések megtétele érdekében feltétlenül szükséges.
>
> (2) A 4. § (1) bekezdése szerinti adatkezelés és adatfeldolgozás esetén az érintett betegségével kapcsolatba hozható minden olyan egészségügyi adat továbbítható, amely a gyógykezelés érdekében fontos, kivéve, ha ezt az érintett írásban kifejezetten megtiltja. Ennek lehetőségéről a továbbítás előtt az érintettet tájékoztatni kell. A 13. § szerinti esetekben az érintett tiltása ellenére is továbbítani kell az egészségügyi és személyazonosító adatot.
>
> (3) A (2) bekezdés szerinti adattovábbítás esetén sem lehet – a 13. §-ban foglaltak kivételével – az érintett hozzájárulása nélkül továbbítani a továbbítás idején fennálló betegséggel össze nem függő, korábbi betegségére vonatkozó egészségügyi adatokat.
>
> (4) Sürgős szükség esetén a kezelést végző orvos által ismert, a gyógykezeléssel összefüggésbe hozható minden egészségügyi és személyazonosító adat továbbítható az érintett hozzájárulása nélkül is.

A 11. § a háziorvos centrális szerepéről szól, alapesetben nála futnak össze a páciensre vonatkozó adatok a különböző ellátóktól. A páciens jogosult arra, hogy a háziorvosa tájékoztassa az egyesített eredményekről. A páciens megtilthatja azt, hogy a kezelőorvosa a háziorvost tájékoztassa. A 12. § biztosítja azt, hogy az ellátó rendszerben megjelent beteg a korábbi egészségügyi adatait önként adhassa meg, annyit, amennyit módjában áll. Vannak olyan esetek, amikor a korábbi egészségügyi adatok átadása kötelező, ezeket az eseteket a 13. § tartalmazza. Fertőző megbetegedés esetén történő kötelező adattovábbítást a 15. § írja le. A 16. § két országos nyilvántartó rendszer működését írja le: a Veleszületett Rendellenességek Országos Nyilvántartásáét (VRONy), illetve a Nemzeti Rákregiszterét. A kezelőorvos köteles adatokat továbbítani ezekbe az adatbázisokba. A 16/A. § a népegészségügyi szűrővizsgálatokhoz kapcsolódó adatkezelést szabályozza. A 19. § az epidemiológiai elemzésekhez szükséges adatok gyűjtéséről, a 20. § a statisztikai adatokról, a 21. § a tudományos kutatások adatkezeléséről, a 22. § a társadalombiztosítási rendszerben az ellátások folyósítása, kiszámítása, elszámolása, és ellenőrzése érdekében szükséges adatkezelésekről szól.

A külső szervek adatkéréséről szól a 23., 24., 25. § szól. A 28. § az adattovábbítási nyilvántartásról szól, a 29. § a betegellátók nyilvántartási kötelezettségéről szól, a 30. § az

adatmegőrzési kötelezettségről, a 31. § az adatok kijavításáról, a 32. § a belső adatvédelmi felelősről, illetve az intézményvezető felelősségéről szól.

5.3. Egyéb egészségügyi jogszabályok

Az Országgyűlés az egészségügyről szóló 1997. évi CLIV. törvényben szabályozta az egészségügyi ellátás jogi alapjait. Ebben a törvényben vannak leírva a betegjogok (dokumentáció megismeréséhez, a másolatkapáshoz, tájékoztatáshoz, a titoktartáshoz, az emberi méltósághoz, az ellátás visszautasításához, az intézmény elhagyásához stb.) A törvény foglalkozik a személyes adatok és a szövetek feletti rendelkezés jogával. A törvény szabályozza a járványügyi intézkedések, a kötelező védőoltások jogszerű módját. Előírja az orvosi dokumentáció vezetését és adattartalmát. A törvény foglalkozik még a szerv- és szövetátültetés, a mesterséges megtermékenyítés, a meddővé tétel szabályozásával.

A nemzeti társadalombiztosítási rendszer által nyújtott szolgáltatások pl. természetbeni egészségügyi ellátás (háziorvos, szakrendelés, kórházi ellátás), gyógyszertámogatás, gyógyászati segédeszköz-támogatás szabályozásával, a támogatás jogosultjaival A kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény (Ebtv.) foglalkozik. A törvény foglalkozik az egyes ellátások tartalmával, a jogosultak körével, illetve a szolgáltatók ellenőrzésével. A törvény szabályozza az elszámoláshoz szükséges adatkezelést, az Országos Egészségpénztár nyilvántartási és adattovábbítási kötelezettségét. A társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény a járulékok kiszámításával, megfizetésével és bevallásával foglalkozik, illetve meghatározza az ezzel kapcsolatos nyilvántartási feladatokat, adatkezeléseket. Az Országos Egészségpénztár a befizetett járulékok személyes adatait nem meghatározott ideig tárolja. Ezt az Alkotmánybíróság nem találta alkotmányellenesnek.

A társadalombiztosítási ellátások igénylésének és igénybevételének módját, a szolgáltatók és a társadalombiztosítás kapcsolatát a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény végrehajtásáról szóló 217/1997. (XII. 1.) Kormányrendelet írja le részletesebben. Az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól 43/1999. (III. 3.) Kormányrendelet az egyes egészségügyi szolgáltatók által jelentett, elszámoláshoz szükséges személyes egészségügyi adatok leírását tartalmazza. Ebben megtalálható a háziorvos, a fogorvos, a fürdőorvos jelentésének a rekordképe a nála megjelent páciensekről, a szakrendelő által jelentett adatok, illetve a fekvőbeteg ellátó intézmények jelentésének rekordképe. A Kormányrendelet foglalkozik a rendszeres finanszírozás pénzügyi kérdéseivel, az előleggel, a téves számlázással, a degresszióval és a teljesítmény-volumen korláttal is. A gyógyszerek, illetve gyógyászati segédeszközök (pl. hallókészülék, szemüveg, járókeret, kötszer) árához adott ártámogatások elszámolásának módját és a kezelt személyes adatok körét A járóbeteg-ellátás keretében rendelt gyógyszerek, gyógyászati segédeszközök és gyógyfürdőellátások árához nyújtott támogatások elszámolásáról és folyósításáról szóló 134/1999. (VIII. 31.) Kormányrendelet tartalmazza.

Az orvosi gyógyszer vények adattartalmát Az emberi felhasználásra kerülő gyógyszerek rendeléséről és kiadásáról szóló 44/2004. (IV. 28.) ESzCsM rendelet tartalmazza. A gyógyászati segédeszközök vényeinek adattartalmát pedig a gyógyászati segédeszközök társadalombiztosítási támogatásba történő befogadásáról, támogatással történő rendelésé-

ről, forgalmazásáról, javításáról és kölcsönzéséről szóló 14/2007. (III. 14.) EüM rendelet. Nemrégen a Parlament módosította az egészségügyi adatok kezeléséről szóló törvényt (Eüaktv.) és megváltoztatta ezeket a miniszteri rendeleteket az Alkotmánybíróság 29/2009. számú határozatának megfelelően. A gyógyszer vényekre nyomtatandó extra vonalkód adattartalmát A gyógyszerrendeléshez használandó számítógépes program minősítésének szabályairól szóló 53/2007. (XII. 7.) EüM rendelet tartalmazza.

Az egészségügyi ellátó rendszerben az EMKI (Egészségügyi Minőségfejlesztési és Kórháztechnikai Intézet, http://www.emki.hu) kapta feladatként a lombikbébi klinikák eredményességének figyelemmel kisérését. A minőségellenőrzés lényegében az eredményességet jelenti, hogy a beavatkozásokat hány esetben követi sikeres gyermekszülés. Az ehhez szükséges adatgyűjtés megvalósítását az emberi reprodukcióra irányuló különleges eljárások végzésére vonatkozó, valamint az ivarsejtekkel és embriókkal való rendelkezésre és azok fagyasztva tárolására vonatkozó részletes szabályokról szóló 30/1998. (VI. 24.) NM rendelet tartalmazza. A rendelet 2008-ban jelentősen megváltozott a páciensek különösen szenzitív adatainak védelme miatt. A korábbi kényszer adatgyűjtés, amely a kezelőlapok és leletek elküldését jelentette az ETT (Egészségügyi Tudományos Tanács, http://www.ett.hu) Humánreprodukciós Bizottsága számára, (amely bizottság egyébként nem fért hozzá a születési adatokhoz, ezért az eredményességet nem tudta nyomon követni) megváltozott. Jelenleg személyes azonosító adatok nélküli adatküldés van csupán, amit nem támogatott esetben meg is lehet tiltani. A születések nyomon követhetőségét egy OEP számára is elküldött kapcsolati kód teszi lehetővé. A minőség-ellenőrzés módját és az eredmények közzé tételének módját a humán reprodukciós eljárásokkal kapcsolatos, kötelezően nyilvánosságra hozandó eredményességi adatok, statisztikák köréről, a nyilvánosságra hozatal módjáról és helyéről, továbbá az ellenőrzés módjáról szóló 339/2008. (XII. 30.) Kormányrendelet szabályozza.

Az orvosi kutatások szakhatósági etikai véleményezését és engedélyezését, ellenőrzését az emberen végzett orvostudományi kutatások, az emberi felhasználásra kerülő vizsgálati készítmények klinikai vizsgálata, valamint az emberen történő alkalmazásra szolgáló, klinikai vizsgálatra szánt orvostechnikai eszközök klinikai vizsgálata engedélyezési eljárásának szabályairól szóló 235/2009. (X. 20.) Kormányrendelet szabályozza.

A Kormányrendelet az orvosi kutatások több változatát különbözteti meg, többféle beavatkozással nem járó vizsgálatot, orvostechnikai eszközzel végzett vizsgálatot, klinikai készítmény (pl. gyógyszer hatóanyag) vizsgálatot, humángenetikai vizsgálatot, illetve az egyéb beavatkozással járó vizsgálatot. Ezeknél más-más szakhatóságok adnak véleményt, illetve más-más hatóságok engedélyezik a kutatást. Meg kell említeni az EEKH (Egészségügyi Engedélyezési és Közigazgatási Hivatalt, http://www.eekh.hu), amely az orvostechnikai eszközök nyilvántartásba vételével, engedélyeztetésével és a velük folytatott kutatások engedélyezésével foglalkozik; illetve az OGYI (Országos Gyógyszerészeti Intézet, http://www.ogyi.hu), amely a gyógyszerek magyarországi forgalomba hozatalára ad engedélyt, illetve engedélyezi az új hatóanyagokkal folytatott orvosi kutatásokat.

A klinikai készítményekkel folytatott kutatások folytatását, engedélyeztetését, ellenőrzését, a kutatási alanyok védelmét az emberi felhasználásra kerülő vizsgálati készítmények klinikai vizsgálatáról és a helyes klinikai gyakorlat alkalmazásáról szóló 35/2005. (VIII. 26.) EüM rendelet tartalmazza, ebben a szó van a kutatás során képződő különleges személyes adatok kezelésének miként jéről. A kutatásban történő részvételbe a páciens önként egyezik bele, és van lehetőség a kutatásból történő kilépésre, illetve a keletkezett adatok

megsemmisítésére. Az orvostechnikai eszközök klinikai vizsgálatáról szóló 33/2009. (X. 20.) EüM rendelet a gyógyászatban felhasználni kívánt új gépekkel, berendezésekkel (pl. lézeres szike, újfajta Röntgen készülék, infrakamera stb.) történő kutatások végzését szabályozza. Az egyéb kutatásokat pedig az általános, az emberen végzett orvostudományi kutatásokról szóló 23/2002. (V. 9.) számú EüM rendelet szabályozza. Ez utóbbiban részletesen le van írva a beleegyezés alaki követelménye, az előzetes tájékoztatás megadásának etikus módja, illetve a humángenetikai törvény által megkívánt külön beleegyező nyilatkozatok formája, ami egyrészt a genetikai mintavételhez, másrészt a biobankban történő elhelyezéshez szükséges.

Különleges személyes adatok kezelését írja elő a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet. A munkavállalók mindegyike rendszeres munkaköri alkalmassági vizsgálatra kötelezett, amelynek során egészségügyi adatok keletkeznek. Ezek további tárolását, kezelését ez a rendelet tartalmazza. A fertőző betegségek és a járványok megelőzése érdekében szükséges járványügyi intézkedésekről szóló 18/1998. (VI. 3.) NM rendelet hozta létre a kötelező védőoltásokban részesített személyek országos nyilvántartását. A korábban csak a kötelező oltásokat tartalmazó adatbázist 2009-ben az országos tisztifőorvos levele alapján kiterjesztették a nem kötelező, H1N1 oltásban részesült személyekre is.

Ellenőrző kérdések

1. Mi a személyes egészségügyi adatok kezeléséről szóló törvény pontos megnevezése?

2. Soroljon fel néhány célt, amelynek érdekében a személyes egészségügyi adatok kezelhetők?

3. Mit tud mondani az egészségügyi adatok kezelésének önkéntességéről?

4. A hozzátartozók megismerhetik-e az elhunyt személy egészségügyi adatait?

5. Milyen feltételek mellett kapcsolhatók össze személyes egészségügyi adatok egymással?

6. A személyes egészségügyi adatok kezelésében mi a háziorvos szerepe?

7. Nem egészségügyi szervek igényelhetnek-e személyes egészségügyi adatokat?

8. Mely törvény szabályozza a betegjogokat és a társadalombiztosítási ellátásokat?

9. Mely hivatal engedélyezi az orvostechnikai eszközökkel végzett kutatásokat?

10. Mely hivatal engedélyezi gyógyszerek forgalomba hozatalát és a velük végzett kutatásokat?

11. Mely jogszabályok foglalkoznak a társadalombiztosítás adatkezelésével?

6. Az Európai Unió jelentősebb adatvédelmi biztosai

A következőkben néhány ismert külföldi adatvédelmi biztos kerül bemutatásra. Elsőként az Egyesült Királyság három utolsó adatvédelmi biztosa. Sorrendben: Elizabeth France (1994-2002), Richard Thomas (2002-2009), végül Christopher Graham (2009-től). Őket a német szövegségi adatvédelmi biztos, illetve a jelenlegi európai adatvédelmi biztos bemutatása követi.

Dr. Elizabeth France

Elizabeth France az Egyesült Királyság Belügyminisztériumában gyakornokként kezdett dolgozni és számos munkakört töltött be. A tisztségéről 1994-ben lemondott és adatvédelmi hivatalvezető lett, majd az 1998-ban elfogadott új adatvédelmi törvény előírásai szerint 1999-től megválasztották adatvédelmi biztosnak. 2001-től az információszabadsággal kapcsolatos feladatokat is ellátta, ugyanis jogszabályváltozás következtében ún. információs biztos lett, pontosabban adatvédelmi és információszabadsági biztos.

Elizabeth France 2002-től az Egyesült Királyság első telekommunikációs ombudsmanja lett. Hivatala az Otelo[36] (Office of the Telecommunication Ombudsman) 2003. január 1-jén nyílt meg. Közreműködött a telekommunikációs törvény elkészítésében, amely 2003-ban, királynői jóváhagyás után megkövetelte minden telekommunikációs szolgáltatótól, hogy működési szabályzatot készítsen. Az üzletszabályzatban, amelyet egy felügyelő hatóság hagy jóvá, a szolgáltatótól megkövetelik, hogy világosan elmagyarázza a panaszok kezelésének menetét, és hogy az ügyfelek a tisztességes kivizsgálás érdekében független testülethez fordulhassanak. Elizabeth France jelenleg igazgatója a Súlyos és Szervezett Bűnözés Ügynökségnek (Serious and Organized Crime Agency). Tagja a Manchesteri Egyetem közgyűlésének, valamint a Walesi Egyetem (Aberystwyth) tanácsának. Amikor adatvédelmi biztosi tevékenységét 2002 júniusában befejezte, munkája elismeréseképpen megkapta a CBE (Commander of the Order of the British Empire[37], a Brit Birodalom Lovagrendjének Parancsnoka) kitüntetést. 2000. július 18-án a Loughboroughi Egyetem tiszteletbeli doktorrá fogadta. Az avatási szertartáson a szónok így méltatta Elizabeth tevékenységét:

> Elizabeth France Loughboroughtól 15 mérföldre nőtt fel. Egyik hobbija a csengők, harangok gyűjtése folyamatos kapcsolatot jelent szülőföldjével, mert a Taylors of Loughborough öntőműhely egyike a két még létező nagy harangöntő műhelynek az Egyesült Királyságban. Elizabeth a Walesi Egyetemen tanult, egy időben Károly herceggel és Neil Hamiltonnal és elnöke volt az egyetemi vitakörnek. 1971-ben politika tudományokból szerzett oklevelet és köztisztviselő lett a Belügyminisztériumban. 1994-ben, 44 éves korában választották meg adatvédelmi hivatalvezetővé.
>
> Miért tekinthetjük Elizabeth Francet az Egyesült Királyság legbefolyásosabb emberének? Önök mindannyian tudatában vannak az információs társadalom gyors fejlődésének. A számítógép használat robbanásszerű elterjedése, az internet, és az

[36] Az Otelo honlapja: http://www.otelo.org.uk/
[37] A CBE kitüntetésről lásd a Wikipedia címszavát: http://en.wikipedia.org/wiki/CBE

elektronikus kereskedelem sohasem látott lehetőségeket teremtettek az emberek számára, hogy teljes körű állampolgárok lehessenek, élethosszig képezhessék magukat, vállalkozzanak, vagy kikapcsolódási lehetőségeket találjanak, (és vagyonokat keressenek vagy veszítsenek el). Azonban az új technológiák nyilvánvaló lehetőséget is nyújtanak arra, hogy kövessék az egyéneket, ahogyan nyomokat hagynak az elektronikus hóban. Ez azt jelenti, hogy mások – lehet, hogy bűnözők, esetleg magándetektívek vagy hitelképesség bíráló cégek, a rendőrség, olyan szervezetek, amelyek valamit el akarnak adni – sokkal többet tudnak a vásárlási szokásainkról, az érdeklődési területünkről és hasonlókról, mint korábban valaha. Nem csak a digitális hálózatokon merülnek fel a magánéletre vonatkozó kérdések. A kamerás megfigyelés a városközpontjainkban és a munkahelyeken ugyancsak azt jelenti, hogy a napjainkat és a napi tevékenységeinket egyre növekvő mértékben figyelik meg.

Ebben a környezetben jelent meg Elizabeth France az első adatvédelmi hivatalvezető. És micsoda hivatalvezetőnek bizonyult! Kezdeményező volt, működése alatt a magánélet, az adatvédelem a politikai életben előkelő helyet kapott. Erőteljes volt a parlament előtti felszólalásaiban, segítséget nyújtott több adatvédelmi tárgyú törvény kialakításához és a hivatala több nagy jelentőségű jogi esetet vállalt fel. Minden eszközzel hangsúlyozza az adatvédelemmel kapcsolatos törvények fontosságát, például:

Az éves jelentésének benyújtásakor szokásos sajtókonferencia helyett 2000. július 12-én elő web közvetítésre cserélte. Augusztusban fizetett reklámkampány indul, hogy felhívja az emberek figyelmét az adatvédelmi jogaikra. (…) Demokráciánk jövőbeli stílusa attól függ, hogy milyen ügyeket vállal fel és melyeket tart elengedhetetlenül fontosnak. Ezért tisztelt kancellár úr, nekem jutott az a megtiszteltetés, hogy bemutathatom Önnek és az egyetemnek Elizabeth France adatvédelmi biztost, hogy kitüntesse a doktor honoris causa címmel.

Elizabeth France egyik legjelentősebb munkája a Use and Disclosure of Health Data (Egészségügyi adatok felhasználása és továbbítása) című útmutató, amely jó néhány évvel megelőzve korát, kimagasló emberiességről, etikai érzékről és a magánélet védelme iránti elkötelezettségről tett tanúbizonyságot. Az Eckstein, S. szerkesztésében készült: Manual for Research Ethics Committees (Kutatásetikai Bizottságok Kézikönyve) egyik fejezete tartalmazza ezt az írást, de szabadon letölthető az angol adatvédelmi biztosi hivatal honlapjáról is.[38] Az Egyesült Királyságban ma is elfogadott és jogalkotási tényező Elizabeth France 1998-as állásfoglalása, amely szerint személyes adatot kutatásra kizárólag akkor lehet felhasználni, ha erről az adatok felvételekor az érintetteket tájékoztatták és azok nem emeltek kifogást.

Richard James Thomas[39]

Az Egyesült Királyság információs biztosa 2002 decemberétől 2009. június 29-ig. A legrangosabb kitüntetése a CBE (Commander of the Order of the British Empire, a Brit Birodalom Rendjének Parancsnoka), amit adatvédelmi biztosi tevékenységéért kapott. Hivatali

[38] Az Egyesült Királyság adatvédelmi biztosi hivatalának honlapja: http://www.ico.gov.uk/
[39] Richard Thomas angol nyelvű életrajza a Wikipédián található, a közölt adatok részben innen származnak: http://en.wikipedia.org/wiki/Richard_Thomas_(lawyer)

idejében sikeresen fellépett a CCTV, a zárt-láncú kamerás megfigyelések terjedése ellen, valamint az Egyesült Királyságban bevezetni szándékozott személyi igazolvány ellen.

1. ábra: Richard Thomas, az Egyesült Királyság korábbi információs biztosa

„A törvényjavaslatban szereplő intézkedések jóval túlnyúlnak azon, hogy létrehozzanak egy biztonságos, megbízható és hiteles személyi kártyát. Az intézkedések, amelyek a nemzeti népesség nyilvántartóval kapcsolatosak, és az állampolgárok személyazonosságának ellenőrzési lehetőségét teremtik meg szükségtelen és aránytalan beavatkozást jelentenek az egyének magánéletébe." – Richard Thomas.

1949 júniusában született egy bíró fiaként. Állami iskolákban tanult majd jogot hallgatott a Southamptoni Egyetemen a hatvanas évek végén. Később jogi tiszteletbeli doktori címet kapott ugyanettől az egyetemtől. Karrierje kezdetén ügyvédgyakornokként, majd ügyvédként, majd később a Nemzeti Fogyasztóvédelmi Tanácsnál dolgozott. Jogi, illetve közönségkapcsolati ügyekkel foglalkozó pozíciókat töltött be 1979-től. Ebben az időszakban részt vett az információszabadságért indított kampányban és részt vett a tudományos közleményekből válogatott Fogyasztási Titkok (Consuming Secrets) c. könyv összeállításában és kiadásában. Richard Thomas jelenleg a Fogyasztók Érdekvédelmi Szervezetének (Consumer's Association) helyettes elnöke, és a tanács meghívott tagja. Megbízott igazgatója a Whitehall & Industry Csoportnak és 2009. szeptember 1-től elnöke a Közigazgatási Igazságszolgáltatási és Bírósági Tanácsnak (Administrative Justice and Tribunals Council). Vendég jogászprofesszor a Northumbria Egyetemen.

1974-ben házasságot kötött Julia Clarke-kal és három felnőtt gyermekük van, Reigateben élnek.

Richard Thomas információs biztosként számos jelentős intézkedést tett, és dokumentumot készített. Az információszabadság törvény végrehajtásához a biztosi hivatal ajánlott fel közzétételi sablonokat különböző adatkezelők számára. A biztosi hivatal elkészítette az Employment Practices Code (Foglalkoztatási gyakorlati jogi útmutató) című ajánlását, a munkavállalók személyes adatainak kezelésére vonatkozóan. Ez a dokumentum számos érdekvédelmi szervezet, érdekelt fél közreműködésével, a vélemények összehangolásával

készült, hasonlóan Elizabeth France munkáihoz. Richard Thomas adta ki a Data Protection Myths and Realities (Adatvédelmi tévhitek és a realitás) című munkáját, amelyben igyekezett egyes adatvédelmi kérdéseket humán nézőpontból megvilágítani.

Christopher Graham[40]

Az Egyesült Királyság adatvédelmi biztosa 2009. június 29-től. 1950. szeptember 21-én született. Kinevezése előtt az Egyesült Királyságban az Advertising Standards Authority (ASA, Reklám Szabályozó Hatóság) elnöke volt. Édesapja, David Graham hosszú időn át ismert újságírója volt a BBC-nek, tudósított a náci haláltáborok felszabadításáról, India függetlenné válásáról, később pedig a kelet-európai eseményekről. Christopher Graham kórista fiú volt a Canterbury Katedrálisban. Később a St. Edwards Iskolában Oxfordban tanult, majd a Liverpooli Egyetem hallgatója lett, és történelemből szerzett diplomát. 1971-72 között az egyetemi hallgatók szervezetének (Guild of Undergraduates) elnöke volt. 1971-74 között Liverpoolban önkormányzati képviselő lett, egyike a legfiatalabbaknak akiket helyi képviselővé választottak az Egyesült Királyságban, mielőtt 2000-ben kinevezték a Reklámhatóság általános igazgatójának. Közben a hetvenes évek közepétől kezdve dolgozott a BBC-nek és titkára volt a BBC kormányzótanácsának (Board of Governors). 1983-ban és 1987-ben mint liberális demokrata jelölt indult a parlamenti választásokon, de nem választották meg.

2. ábra: Christopher Graham, az Egyesült Királyság jelenlegi információs biztosa

Peter Schaar

Berlinben született 1954-ben, házas két gyermeke van. 2003. december 17-e óta német szövetségi adatvédelmi biztos. Ezen kívül az EU adatvédelmi irányelv 29. cikke alapján megválasztott munkacsoport elnöke, többször egymás után is megválasztották erre a tiszt-

[40] Christopher Graham angol nyelvű életrajza a Wikipédián található, itt egy rövid magyar részlet található: http://en.wikipedia.org/wiki/Christopher_Graham

ségre. Közgazdasági diplomájának megszerzése után 1980 és 1983 között Hamburg szabad Hanzaváros önkormányzatánál a közigazgatásban dolgozott. Később az adatfeldolgozási és statisztikai részleg vezetőjeként folytatta tevékenységét. 1986 és 1994 között a hamburgi adatvédelmi biztos hivatalánál volt részlegvezető, majd később 1994-től 2002-ig helyettes biztos. 2001 és 2002-ben részt vett az adatvédelmi törvény modernizálását célzó bizottság munkájában. 2002-ben saját magán adatvédelmi tanácsadó céget alapított Hamburgban, amelynek ügyvezető igazgatója volt 2003-ig. Tagja a Gesellschaft für Informatiknak (Informatikai Társaság), az International Working Group on Data Protection in Telecommunications (IWGDPT, Nemzetközi Munkacsoport a Telekommunikáció Adatvédelmére), és a Hamburger Datenschutzgesellschaftnak (HDG, Hamburgi Adatvédelmi Társaságnak), valamint a Humanistische Unionnak (Humanista Egyesület).

2006. január 1.-je óta német szövetségi adatvédelmi biztos. Két könyvet is írt: Adatvédelem az Interneten. Az alapok. címmel 2002-ben, illetve a Magánszféra vége, út a megfigyelő társadalom felé 2007-ben jelentek meg. A nevéhez fűződik az a híres mondás: „*A legjobb adatvédelem, az adatkezeléstől való tartózkodás.*" Peter Schaar az európai kontinensen először javasolta a német parlamentnek, hogy módosítsák úgy az adatvédelmi törvényt, hogy az adatkezelések során fellépett incidenseket az adatkezelő köteles legyen nyilvánosságra hozni. A törvénymódosítás 2009. szeptember 1-jén lépett hatályba.[41] Jelenleg ugyanis az incidenseket az adatkezelők eltitkolják és az érintettek nem szereznek tudomást az adatvesztésről, adatlopásokról.

Peter Hustinx

2004 óta dolgozik, mint EDPS (European Data Protection Supervisor, Európai Adatvédelmi Biztos). Jogállását tekintve az európai adatvédelmi biztos az Európai Közösség központi szervezetei által kezelt adatok védelméért felelős, részt vesz a 29. munkacsoport munkájában, illetve ajánlásokat bocsáthat ki az EU adatvédelmi irányelvének egységes alkalmazása ügyében az Európai Parlament és a tagállamok számára. Ugyanakkor nem tekinthető a nemzeti adatvédelmi hatóságok felettes hatóságának. Peter Hustinx részt vett az új EU biztosi hatóság[42] felállításában és közösségi szintű szerepének fejlesztésében. 2009 januárjában újabb ötéves hivatali periódusra megválasztották. Megválasztása előtt, Peter Hustinx a holland adatvédelmi hatóság elnöke volt 1991 óta, majd 1996 és 2000 között a 29. cikk alapján megválasztott munkacsoport elnöki tisztségét is betöltötte. Korábbi sikeres adatvédelmi tapasztalatát most európai szinten folytatja. Szakértőként vett részt az ETS-108 számú Strasbourgi Egyezmény elkészítésében, amelyet az Európa Tanács hozott tető alá, büntető jogi területen is rendelkezik tapasztalatokkal, mivel az Európai Rendőrség, az Europol Egyesített Felügyeleti Testülte Fellebbviteli Bizottságának, valamint az Interpol Aktákat Felügyelő Bizottságának az elnöke is volt.

Mint európai adatvédelmi főbiztos az Európai Unió hivatalos lapjában közzé tette véleményét az Európai Parlament és Tanács által tervezett, a határon átnyúló egészségügyi ellátásokra vonatkozó betegjogok érvényesítéséről szóló irányelvéről (Európai Unió Hivatalos Lapja, 2009/C, 128, 20-27. oldal). Peter Hustinx adatvédelmi főbiztosi minőségében

[41] BNA International, World Data Protection Report: The German Federal Data Protection Act and its recent changes

[42] Az Európai Adatvédelmi Biztos Hivatalának honlapja: http://www.edps.europa.eu/

egy angol nyelvű útmutatót bocsátott ki az Európai Unió közösségi intézményeinek munkahelyein dolgozó személyek egészségügyi adatainak kezelése ügyében. Felszólalt az emberi, illetve állatgyógyászati felhasználásra szánt gyógyszerek engedélyezésére és felügyeletére vonatkozó közösségi eljárások meghatározásáról és az Európai Gyógyszerügynökség létrehozásáról szóló 726/2004/EK rendelet tervezetével kapcsolatban és kénytelen volt megállapítani, hogy a tervezett gyógyszer mellékhatás adatbázis semmilyen adatvédelmi intézkedéseket nem tartalmaz, holott azonosítható személyek bizalmas egészségügyi adatait kívánja összegyűjteni (Európai Unió Hivatalos Lap, 2009/C 229/04).

Ellenőrző kérdések

1. Mikortól nevezték információs biztosnak az Egyesült Királyság adatvédelmi biztosát?
2. Sorolja fel a három utolsó információs biztost az Egyesült Királyságban!
3. Milyen úttörő kezdeményezései voltak Elizabeth Francenak?
4. Ismertesse röviden Richard Thomas életútját és fontosabb munkáit?
5. Ismertesse röviden Christopher Graham életútját!
6. Ismertesse a jelenlegi német szövetségi adatvédelmi biztos életútját és fontosabb kezdeményezéseit!
7. Mi a feladata az Európai Adatvédelmi Biztosnak, ki töltötte be ezt a pozíciót 2010-ben?

7. Az Európai Unió által támogatott adatvédelmi kutatási projektek

A következőkben néhány európai uniós kutatási projekt kerül bemutatásra, amelyek céljai között adatvédelmi kérdések is szerepeltek. Ezek a projektek alapvetően a 95/46/EK adatvédelmi irányelv nemzeti megvalósításait, és a felmerülő problémák különböző megoldásait kutatták. A projektek eredményeként ajánlásokat tettek az adatvédelmi irányelv egységes alkalmazásának elősegítésére, az egyelőre nem megoldható kérdéseket pedig rögzítették a jövőbeli feladatok között.

7.1. A PRIVIREAL FP5 projekt

Az Európai Unió FP5 kutatási programjának támogatásával jött létre a PRIVIREAL (Privacy in Research Ethics and Law, A magánélet védelme a kutatásetikában és a törvényekben) kutatási projekt. A projekt három és fél évig tartott (42 hónap), 2002 januárjától 2005 júniusáig. A alapvető célja az volt, hogy megvizsgálja a 95/46/EK adatvédelmi irányelv nemzeti megvalósításait az orvosi kutatásokban és a kutatásetikai bizottságok szerepét. Magyar részről Dr. Sándor Judit, egyetemi tanár, a Közép-Európai Egyetem munkatársa vett részt a projektben.

A PRIVIREAL projekt céljai részletesebben:

- Létrehozni és működtetni egy web alapú erőforrást, amely információkat szolgáltat arról, hogy egy-egy tagállam hogyan valósította meg a 95/46/EK adatvédelmi irányelvet, különösen az orvosi kutatások területén. Minden egyes ország adatlapján az aktuális adatvédelmi törvények és szabályozások megtalálhatók, valamint kommentárok és más háttér információk. A hivatkozásokat tenni első sorban a partnereink adatvédelmi törvényeire, de további kiegészítő információkat is közzé lehet tenni olyan államok adatvédelmi törvényeire, amelyek nem vesznek részt a projektben.
- Megvizsgálni a tagállamokban a független etikai bizottságok etikai véleményezését az adatvédelem szempontjából. Ennek érdekében információkat gyűjteni arról, hogy a törvénykezés hogyan befolyásolja az etikai bizottságokat, amikor azok véleményt alkotnak egy-egy kutatási tervről.
- Végül, ajánlásokat kidolgozni azzal kapcsolatban, hogy a tagállamokban hogyan kellene alkalmazni a 95/46/EK adatvédelmi irányelvet, és egy visszajelzést adni az etikai bizottságoknak arról, hogy az adatvédelmi irányelv alapján hogyan kellene a kutatások résztvevőinek jogait védeni.

A projekt koordinátorai Deryck Beyleveld professzor és David Townend a Sheffieldi Egyetemről. A projekt workshopok megrendezését a finn és portugál partnerek segítették. Az Európai Bizottság szerződésének száma: No. PL QLRT-2001-00056, by the European Commission, DG Research, Directorate E: Biotechnology, Agriculture and Food, FP5, Quality of Life Program.

A projekt honlapja: http://www.privireal.org/

A projektben 49 egyéni és intézményi résztvevő volt 27 országból, beleértve az Európai Unió új tagállamait és tagjelölt államait. Három workshop került megrendezésre: 2003. januárjában Sheffieldben, 2003. augusztusában Helsinkiben, 2004. júliusában Coimbrában. A projekt eredményeiből a tervek szerint öt könyv készül, amiből eddig három már megjelent, és amelyek a projekt három mérföldkövének eredményeit tartalmazzák.

7.2. Az EuroSOCAP FP6 projekt

A projekt célja egy a páciensek személyes egészségügyi adatainak kezelésére vonatkozó szabványt kidolgozása volt, amely elsődlegesen etikai alapokon nyugszik, ugyanakkor az érvényes európai szabályozásnak megfelelően jogilag is alátámasztott.

A bizalmas adatkezelésre és a magánélet tiszteletben tartására kidolgozott európai szabvány az EuroSOCAP (European Standards On Confidentiality And Privacy in healthcare) projekt (QRLT-2002-00771) során készült. Az EuroSOCAP egy az Európai Bizottság által támogatott projekt volt 2003 és 2006 között, amely abból a célból jött létre, hogy a szakma szembesüljön és válaszoljon azokra az egészségügyi szektorban keletkezett kihívásokra és feszültségekre, amelyek az információ vagy tudásalapú társadalom és az egészségügyi információk bizalmasságának és a magánélet tiszteletben tartásának alapvető jogi és etikai követelményei között keletkeztek.

A Szabvány minden egészségügyi szakemberre és egészségügyi ellátó intézményre vonatkozik és kiterjed az egészségügyi ellátás bizalmas adatkezelésének és a magánélet tiszteletben tartásának különböző területeire. A project résztvevői kimunkálták a szabvány etikai és jogi alapjainak hátterét, útmutatást adnak az egészségügyi szakemberek számára a leghelyesebb etikai gyakorlatra vonatkozóan és ajánlásokat fogalmaznak meg az egészségügyi ellátó intézmények számára.

Az európai szabvány elsősorban etikai szabvány. A résztvevők áttekintették az egészségügyi szakemberek európai törvényi kötelezettségeit és azt az általános jogi környezetet, amelyben a bizalmas információk védelméről, felhasználásáról és továbbításáról szóló szakmai döntések történnek. Ennek az etikai útmutatónak a jogi környezetét olyan jogi alapelvek és rendelkezések jelentik, amelyek betartathatók Európában (mint például az EU 95/46/EK számú adatvédelmi irányelve és az Emberi Jogok Európai Egyezménye). Ezek a rendelkezések nem merülnek ki abban, hogy kötelezővé teszik az egészségügyi szakemberek számára a páciensek magánéletének tiszteletben tartását és bizalmas adatainak védelmét. Esetenként az egészségügyi szakembereknek a gyakorlatban szükségük lehet arra is, hogy szakmai véleményt alkossanak. Ez a szabvány etikai útmutatást nyújt minden egészségügyi szakember számára egy ilyen vélemény kialakításához. A legjobb etikai gyakorlat is igényel egy támogatást nyújtó környezetet, ezért a szabvány ajánlásokat is tartalmaz az egészségügyi ellátó szervezetek számára azokkal az intézkedésekkel kapcsolatban, amelyek a gyakorlatban szükségesek a szabvány leghatékonyabb megvalósításához.

A szabvány írásakor különös figyelemmel voltak a kiszolgáltatott helyzetben lévő páciensek speciális igényei iránt — különösen a gyerekek, a fiatalok, az idősek, a bevándorlók és a vándorló életmódot folytatók, az elítéltek, a hajléktalanok, a mentális egészségügyi problémával küszködők, a csökkent szellemi képességűek, és az olyan személyek iránt, akik nem rendelkeznek önálló döntéshozási képességgel. A kiszolgáltatott helyzetben lévő páciensek magánéletének és egészségügyi adatai védelmének speciális kockázati tényezői-

re történő határozott koncentrálás nagymértékben befolyásolta az általános Szabvány kialakítását, hogy útmutatót adhasson azoknak az egészségügyi szakembereknek is, akik működésük során kiszolgáltatott helyzetű páciensekkel kerülnek kapcsolatba.

A Szabvány és az Útmutató különböző nyelveken elérhető a http://www.eurosocap.org weblapon.[43] A weboldal ezen kívül még tartalmaz: az egészségügyi adatkezelés és titoktartáshoz kapcsolódó érdeklődési területekről újdonságokat; kereshető adatbázist a releváns szakirodalom webcímeivel, valamint egy kereshető adatbázist is tartalmaz szakértők és érdeklődő partnerek adataival egész Európa területéről.

A projektben 20 tag vett részt — klinikusok (különböző szakterületek képviselői), orvosok, jogi szakértők és etikusok Európa 11 országából. A Szabvány előzetes verzióját a projekt résztvevői egy több mint két éves periódus alatt készítették el (további hat meghívott szakértő közreműködésével). Ezután a Szabvány előzetes verzióját széles körben terjesztették további konzultáció céljából 2005-ben, illetve ez volt a témája annak a Workshopnak, amelyen 80 szakértő vett részt 26 európai és szomszédos országból. Sokféle válasz érkezett a konzultáció folyamán, amelyek között megjelentek a pácienseket képviselő szervezetek, nemzeti orvosi szervezetek, nemzeti egészségügy minisztériumok, nemzeti adatvédelmi szervezetek, az Európai Bizottság, az ipar, az egyetemek és mértékadó nemzetközi szervezetek nézőpontjai. E konzultációs folyamat alapján egy átdolgozott előzetes Szabványt készítettek és küldtek szét a konzultáció egy következő fordulójában. A Szabványt az EuroSOCAP projekt vezető testületének tanácskozásán véglegesítették 2005 novemberében.[44] A szabvány magyar nyelvű változatát Dr. Alexin Zoltán fordította magyar nyelvre, miután 2006-ban meghívták a projekt résztvevői külső szakértőnek.

7.3. A SENIOR FP7 projekt

A SENIOR (Social, Ethical and privacy Needs in ICT for OldeR people, Az idősödő személyek szociális, etikai és magánéleti igényei az infokommunikáció korában) projekt az Európai Bizottság támogatásával jött létre számos nemzetközi résztvevő intézmény és egyéni kutató részvételével 2008 és 2009 között (24 hónap).

A világon a népesség gyorsan öregszik: a 60 év feletti populáció aránya a társadalomban meg fog duplázódni. 2006-ban 11% volt, míg 2050-re ez az arány 22% lesz. Akkora több idős ember lesz, mint 0-14 éves gyerek először az emberi történelemben. Európa lakossága még rohamosabban öregszik, aminek jelentős negatív hatása van gazdasági növekedésre.

Mérnökök és politikusok tudják, hogy az infokommunikációs technikák (ICT, Information Communication Technologies) drámaian meg tudják változtatni az idős emberek életkörülményeit, és az öregedést a gazdasági tehertétel helyett egy potenciálisan produktív erőforrássá változtathatják. Jelenleg még két tényezője van az ICT eszközök korlátozott használatának. Először, az idős emberek gyakran kellemetlen érzéseket táplálnak az ICT iránt, amely túlságosan távol van attól a világtól, amelyben megszokták, hogy élnek. Másodszor, az ICT eszközöket gyakran úgy tervezik, hogy nem veszik figyelembe az idős emberek kisebb nehézségeit. Ez a helyzet most meg fog változni. A világháború utáni ge-

[43] Sajnos a projekt vége után két évvel a weboldal elérhetőségét megszüntették. A dokumentumok nem vesztek el. Az angol eredeti és a lefordított magyar verzió megtalálható a: http://www.tisztessegesadatkezeles.hu/hirek-cikkek/az-eurosocap-fp6-projekt.html weboldalon.
[44] A szabvány letölthető a következő webcímről: http://www.orpha.net/testor/doc/july05/EuroSOCAP.pdf.

neráció, amely a legnagyobb a történelemben elérte a 60 éves kort és sokkal képzettebb, mint az előző generációk. A következő évek bizonnyal az „informatika az idősödő emberek számára" jelszó jegyében telnek, amikor felismerik, hogy a kommunikációs és információs szolgáltatásokhoz való hozzáférés az idősödő polgártársaink lényeges emberi joga. Ez azonban különböző kihívásokat jelent, néhány ezek közül az ICT eszközök mindenki számára azonos módon történő tervezésével és megvalósításával kapcsolatosak, míg mások etikai és magánéleti kérdésekkel. Az ICT eszközök elterjesztését sok esetben a költséghaszon megfontolások irányítják, ugyanakkor az ICT a magánéletre háborítatlanságára, a szabadság, a méltóság, autonómia és más alapvető etikai normák tiszteletben tartására vonatkozó kérdéseket vet fel. A probléma kiterjedtségének érzékeltetésére, elég arra a technológiára gondolnunk, amelynek széles körű elterjedése már elkezdődött, ami egy viselkedési mintákat monitorozó rendszer. Az idősödő személyek viselkedését megfigyelik, és minden változást jelentenek a gondozóknak; az ajtókon szenzorok vannak, amelyek figyelmeztetést adnak minden szokatlan nyitás esetén, elektronikus RFID jeladókat viselnek, amelyek lehetővé teszik az idős személyek helyzetének a meghatározását, és így tovább. Azért jött létre ez a projekt, hogy létrehozza azokat a kereteket, amely szükségesek azoknak az etikai és személyiségvédelmi kereteknek a létrehozásához, amelyek védik az idősödő generációt az ICT-vel kapcsolatos visszaélésektől, jogsértésektől.

A projekt adatai:

A SENIOR projekt 24 hónapos működése alatt támogatott minden olyan kezdeményezést, amelynek a célja, hogy szisztematikusan felmérje az idősödő generáció szociális, etikai és magánéleti problémáit az ICT alkalmazásával kapcsolatban hogy megérthessük, mit kell megtanulnunk a jelenlegi gazdasági trendekből, és hogy stratégiákat dolgozhassanak ki a jövő irányaira nézve. A SENIOR konzorcium elkötelezett arra, hogy megvizsgálja, hogy az új ICT technológiák hogyan elégíthetik ki az idősödő emberek igényeit anélkül, hogy kompromisszumokat kellene kötni az etikai és személyiségvédelmi kérdésekben. Három fő alapelven nyugszik a projekt, amelyek meg is határozzák a mérföldköveit: célja a párbeszéd, eszköze a vita és a megbeszélés, a technológiai tervezés a végcél.

A SENIOR része egy szélesebb körű EU stratégiának, amelyet a Lisszaboni Egyezmény alapozott meg, és amelynek célja a szegénység és a szociális kirekesztettség felszámolása 2010-re. A 2006-os rigai miniszteri nyilatkozat hat témát határozott meg, amely elősegíti az elektronikus társadalmi integrálódást (e-Inclusion): az általános hozzáférés (e-Accessibility); az idősödő személyek képessé tétele arra, hogy teljes mértékben részt vegyenek a gazdaságban és a társadalomban (e-Ageing); a társadalom tagjainak felruházása minden tudással és képességgel arra, hogy élethosszig tanuljanak (e-Competences); Szoci-Kulturális e-Inclusion, a kisebbségek, a bevándorlók, és a perifériára szorult fiatalok bevonása; Földrajzi e-Inclusion, fejleszteni a szociális és gazdasági jólétet a gazdaságilag hátrányos területeken az ICT segítségével; részvételi e-Government, növelni közösségi részvételt a demokráciában.

A SENIOR projekt hozzájárulása a fenti célkitűzésekhez kettős. Először, a SENIOR rögzíteni fogja az ICT-nek az etikára és a magánéletre gyakorolt hatásait az elektronikus integrációban. Ezt a célt tematikus szakértői értekezletekkel kívánja elérni. Minden egyes tanácskozás (i) rendszer szintű ICT megoldásokat és trendeket határoz meg, és (ii) megvitatja a releváns etikai és magánéleti kérdéseket, és (iii) értékeli a technológiai fejlesztés, valamint az etika és a személyiségvédelem területén hozott kompromisszumokat. Másodszor, a projekt meghatározza azokat az ICT szolgáltatásokat, amelyek segítik az elszigete-

lődés elkerülését, és segítik az idős emberek integrálódását. A projekt egy munkatervet hoz létre, amelyet figyelembe lehet venni a későbbi technológiai tervezésben, kulcsfontosságú lépéseket, befektetési stratégiát, erőforrás igényt, kockázatbecslést és mérföldköveket fog tartalmazni.

Várható eredmények:

A fő eredmény egy 2020-ig terjedő munkaterv, amely a várakozás szerint meghatározza az ICT jövőbeni fejlesztését és eljuttatását az idősödő személyekhez Európában. A projekt honlapja: http://www.seniorproject.eu/[45] A projektnek nem volt magyar résztvevője. A brüsszeli projektindító tanácskozáson azonban Dr. Alexin Zoltán részt vett.

7.4. A RISE FP7 projekt

A RISE projekt (Rising pan-European and International Awareness of Biometrics and Security Ethics, A pán-európai és nemzetközi figyelem felkeltése a biometria és a biztonság etikája iránt) egy nemzetközi kezdeményezés, amely feladata a biometriai és biztonsági technológia etikájával kapcsolatos tudatosság elősegítése. A projekt elmélyíti, kibővíti és folyamatosságot biztosít annak a európai és nemzetközi párbeszédnek, amely az EC DG Research (European Commission Directorate General – Európai Bizottság Kutatási Főigazgatóság) és US DHS Privacy Office (United States, Department of Homeland Security, Egyesült Államok Belbiztonsági Szolgálat, Személyiségi Jogi Irodája) által Brüsszelben és Washington DC-ben2005-ben és 2006-ban szervezett etikai és biometriai nemzetközi konferenciák után már megindult.

A RISE egy36 hónapos Coordination and Support Action (CSA) FP7 projekt. A szerződés száma: 230389

A projekt elképzelései:

A modern fenyegetések elleni harc és a hatékony biztonsági intézkedések, különösen a biometrikus technológia területén együttműködést igényel, és nemzetközi párbeszédet a fő szereplők között, nevezetesen az Európai Unió, az Egyesült Államok és Ázsia között. Hogy megteremtsük a bizalmat és a kölcsönös megértést a párbeszédbe be kell vonni a fő érdekelteket, akik különböző tudományterületeket képviselnek, és különböző filozófiai, politikai és vallási nézőpontokat. Hisszük, hogy egy világméretű kutatás, a nemzetköziség, és a sokféleség a kulcs a sikeres megközelítési mód a biometrikus politika kialakításához a nemzetközi arénában.

Háttér

Egy nemzetközi párbeszéd kezdődött el az etikai és biometriai kérdésekről az Európai Unió Kutatási Főigazgatósága (konferencia 2005-ben) és az Egyesült Államok Belbiztonsági Szolgálata (konferencia 2006-ban) szervezésében a BITE (Biometric Identification Technologies Ethics, A biometrikus azonosítási technológiák etikája) FP6 keretprogram egy projektjének[46] keretein belül. Az Európai Bizottság 2008-ban támogatott egy kutatási projektet, amely speciálisan a biometria etikájával és bevezetésével, valamint személydetektálási technológiákkal foglalkozott. A HIDE (Homeland security, biometric

[45] A SENIOR projekt 2009. december 31-én ért véget.
[46] A BITE projekt 2007. február 27-én véget ért. Honlapjának címe: http://www.biteproject.org

identification and personal detection ethics, A belbiztonság, a biometriai azonosítás, a személy detektálás etikai kérdései) projekt[47] kikövezte az utat a RISE projekt számára, azzal, hogy a technológiai környezetre helyezte a fő hangsúlyt.

A projekt küldetése

A RISE projekt összefoglaló célja, hogy elmélyítse és bővítse azt a nemzetközi és európai párbeszédet, ami a biometriai és a biztonságtechnológiai intézkedésekről és annak etikájáról indult 2005-ben. A további speciális célkitűzések között található két nemzetközi konferenciasorozat és egy sor regionális tanácskozás szervezése.

A projekt honlapja: http://www.riseproject.eu

Ellenőrző kérdések

1. Mik volt a PRIVIREAL európai projekt céljai?
2. Milyen célt tűzött ki az EuroSOCAP projekt maga elé és mit valósított meg ebből?
3. Jelent-e kötelezettséget a tagállamokra az EuroSOCAP szabvány?
4. Milyen megközelítést alkalmazott az EuroSOCAP szabvány a magánélet védelmére?
5. Milyen társadalmi probléma vizsgálatát tűzte ki célul a SENIOR projekt?
6. Az idősödő generációt milyen módon tervezi integrálni a társadalomba a SENIOR projekt?
7. Miért merülnek fel etikai és a magánélet védelmével kapcsolatos társadalmi kérdések az idősödő generáció integrációjakor?
8. Milyen eredményei voltak a SENIOR projektnek?
9. Mi a RISE FP7 projekt célja?
10. Mondjon példákat olyan etikai kérdésekre, amelyekkel a RISE projekt foglalkozik!

[47] A HIDE projekt honlapja: http://www.hideproject.eu

8. A tudományos kutatások adatkezelésének etikai alapelvei

Az EU 95/46/EK számú adatvédelmi irányelve kimondja, hogy személyes adatokat csak előre meghatározott, törvényes célból lehet kezelni és a későbbiekben kizárólag az eredeti célokkal kompatibilis célokra lehet az adatokat felhasználni. Az Európai Bizottság azonban kimondta, hogy a tudományos kutatási célú felhasználás kompatibilis bármilyen más adatkezelési céllal, és egyben törvényes célnak tekinthető. Ezzel lehetővé vált a személyes adatok felhasználása tetszőleges kutatási célra. A kutatási célokat, érdekeket egyedül az érintettek adatvédelemhez fűződő jogai, illetve a kutatókra vonatkozó etikai szabályok korlátozzák. Formalizált etikai felügyelet egyedül az orvosi kutatások esetén figyelhető meg. Itt egy etikai bizottságnak kell támogatni a kutatási tervet ahhoz, hogy a kutatás megvalósulhasson. Más szakmákban formalizált etikai követelményrendszer nem ismert.

Az Avtv. rendelkezéseiből következik, hogy adatkezelésre vagy önkéntes hozzájárulás, vagy egy törvény előírása alapján kerülhet sor. Már ez a körülmény is jelentős morális és etikai problémát vet fel. Ugyanis, ha nincs erre vonatkozó törvény, akkor nehéz minden esetben a hozzájárulást megszerezni. Másrészt, amikor törvény alapján kerül sor az adatkezelésre, akkor pedig gyakorlatilag kényszer kutatásra kerül sor. Személyes adatoknak a halál után történő felhasználása tekintetében a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény ad útmutatást. Eszerint a halál után 30 évvel válik kutathatóvá egy levéltári dokumentum, ha a halál időpontja nem ismert, akkor a születéstől számított 90 évvel, ha a születési idő sem ismert, akkor a dokumentum keletkezésétől számított 60 évvel. Azonban ennél korábban is adnak engedélyt kutatásra, amennyiben a kutató írásban kötelezettséget vállal az Avtv. rendelkezéseinek betartására – ami gyakorlatilag azt jelenti, hogy nem hozza nyilvánosságra a megismert adatokat személyazonosításra alkalmas formában. Az adatvédelmi törvény szerint a történelmi események jobb megértésének céljából a kutató személyes adatokat is nyilvánosságra hozhat a saját mérlegelése alapján. Itt az érintettek adatvédelemhez fűződő jogai ellentétbe kerülhetnek a történelem megismeréséhez fűződő társadalmi érdekkel.

Tudományos kutatások során is adatkezelés történik, amellyel szemben a korábban említett nyolc adatvédelmi alapelv (minimálisan szükséges adatmennyiség, célhoz kötött adatkezelés, hozzáférés, kijavítás, másolat biztosítása, törléshez való jog, …) közül a tisztességességnek jut nagy szerep. Elizabeth France a tisztességességet abban látta, hogy az érintetteket mennyire részletesen tájékoztatják *az adatkezelés előtt* az adatkezelés főbb jellemzőiről, a jogaikról. Az adatkezelés alapelveit a 95/46/EK adatvédelmi irányelv 6. cikke gyűjti össze. A IV. Fejezet 10. cikkelyében további kötelezettségeket állapít meg az adatkezelőkre vonatkozóan, mely szerint bizonyos információkat át kell adniuk a személyes adatok felvételekor az érintetteknek (vö. Avtv. 6. §.):

- az adatkezelő megnevezése;
- az adatkezelő képviselője, ha ilyen személy létezik, akit erre a célra az Avtv. és az Eüaktv. szerint kijelöltek (vö. belső adatvédelmi felelős);
- melyek azok a célok, amelyek érdekében a személyes adatokat feldolgozzák;
- egyéb további információk, amelyek szükségesek figyelembe véve, azokat az egyedi körülményeket, amelyek során az adatokat feldolgozzák, vagy fel fogják dolgozni, hogy ezzel biztosítsák az érintett szemszögéből nézve a feldolgozás tisztességességét.

Ezeket a részleteket gyakran nevezik „tisztességes adatkezelési információknak", „a tisztességes feldolgozás szabályának" vagy a „tisztességes adatgyűjtés szabályának".[48] Az Egyesült Királyság parlamentje mellett működő POST (Parliamentary Office of Science & Technology, tudományos és technikai parlamenti iroda) rendszeresen készít a Parlament számára háttér anyagokat, amelyek az interneten elérhetők.[49] 2005-ben két dokumentum is készült, az orvosi kutatásokkal kapcsolatban: a 235-ös számú dokumentum a Data Protection in Medical Research (Adatvédelem az orvosi kutatásban), a 243-as dokumentum az Ethical Scrutiny of Research (A kutatások etikai elbírálása). E dokumentumokban ugyancsak megjelent az, hogy a tisztességes adatkezelés *feltétele* az érintettek előzetes tájékoztatása.

A 29. cikk alapján létrejött munkacsoport a 2008-ban kiadott WP148 számú munkadokumentumában foglalkozott az internetes szolgáltatások (alapvetően a webes kereső szolgáltatások) adatkezelésével. A munkacsoport ugyancsak megállapította, hogy az adatkezelő tájékoztatási kötelessége egyike az adatkezelés alapvető feltételének, amelyez az EU 95/46/EK adatvédelmi irányelvének 10. §-a ír le, amikor az adatokat közvetlenül az érintettektől szerzik be. A 10. § szerint az adatkezelőnek következő információkat kell előzetesen biztosítani:

- az adatkezelő és képviselőjének megnevezése; ha van ilyen;

- az adatkezelés lehetséges céljai, amelyhez az adatokra szükség van;

- további információk, mint

- további adatátvevők, vagy az adatátvevők kategóriái, akikhez az adatokat továbbítják;

- az adatok megadása önkéntes vagy kötelező, illetve a válaszadás megtagadásának következményei;

- az érintetteknek joga van a rájuk vonatkozó adatokhoz hozzáférni és kérni a kijavításukat.

A webes szolgáltatások esetén az adatkezelő kötelessége, hogy egyértelművé tegye: milyen adatokat gyűjt a felhasználókról és azokat mire használja. Amikor adatokat gyűjtenek, minden esetben egy egyszerűbb tájékoztatást kell adni az adatok felhasználásáról, még akkor is, ha máshol egy részletes leírás áll rendelkezésre. A felhasználókat tájékoztatni kell a sütikről is, amelyeket a szolgáltatás a helyi számítógépen elhelyez, és hogy hogyan lehet ezt elkerülni, vagy a sütiket később törölni. A munkacsoport úgy tartotta, hogy ezek az információk szükségesek ahhoz, hogy egy webes szolgáltatás a tisztességes adatkezelést garantálja.

A technikai fejlődés eredményeként az elmúlt években hatalmas mennyiségű személyes egészségügyi adat gyűlt össze az államok ellátórendszerében az elektronizálás következtében, illetve a társadalombiztosítási rendszerekben. A polgárok személyes egészségügyi adatainak összekapcsolt elektronikus tárolása, és kutatásra történő felhasználása a közeljövő fontos emberi jogi problémája lesz. Az adatkezelés jelenleg az ellátórendszerekben egyre inkább nem elégíti ki az adatvédelem máshol szokásos alapelveit; sem a minimálisan szükséges adatmennyiség elvét, sem azt az elvet, hogy a lehető legrövidebb ideig tárolják az adatokat személyazonosításra alkalmas formában, sem a transzparencia elvét, illetve azt,

[48] Elizabeth France: Use and Disclosure of Health Data
[49] A POST honlapja: http://www.parliament.uk/business/publications/research/post/

hogy az adatkezelés alapvetően önkéntes alapon történjen. Ilyen háttér esetén az egész adatkezelési folyamat tisztességessége, valamint egy beleegyezés nélküli kutatások lehetősége komoly vitákat fog még kiváltani. Ezért a következőkben az orvosi kutatásokra vonatkozó alapvető etikai és adatkezelési szabályokat tekintjük át.[50]

8.1. Az orvosi kutatások adatvédelmi feltételei

Az Avtv. szerint, amennyiben egy adatkezelést törvény rendel el, akkor annak a törvénynek szabályoznia kell, az adatok felvételének lehetséges céljait, az adatokhoz történő hozzáférést, a tárolás idejét. Az egészségügyi adatok esetében ez a törvény az 1997. évi XLVII. Az egészségügyi adatok kezeléséről szóló törvény (Eüaktv.). A törvényben nem szabályozott általános esetekben pedig az adatvédelmi törvény rendelkezéseit kell alkalmazni.

Az Eüaktv. rendelkezik arról, hogy milyen célokra lehet egészségügyi adatokat felvenni, az egészségügyi adatok felvételekor hogyan kell eljárni, az adatokat hogyan lehet továbbítani, hogyan lehet összekapcsolni, kik ismerhetik meg az adatokat, és meddig kell azokat megőrizni. Az Eüaktv. szerint gyógykezelés, az egészségi állapot nyomon követése, kutatás stb. célokból lehet személyes egészségügyi adatokat felvenni, így teljesül az Avtv. azon elvárása, hogy személyes adatokat csak törvényben előre felsorolt célból lehet felvenni. Az Avtv. 6. §-a előírja, hogy az adattárolás céljait még az adatfelvétel előtt a pácienssel megismertessék. Miért van erre szükség?

Az orvosi kutatásokban a pácienseknek nem kötelező részt venniük. Ha nem kívánnak benne részt venni, gyakorolhatják a kimaradás jogát (opt-out), amely az Avtv. 16/A § (2) bekezdésében szerepel. Ez azt jelenti, hogy amikor közlik a pácienssel, hogy adatait esetleg kutatásra is igénybe kívánják venni, akkor közölheti, hogy hozzájárul-e ehhez, vagy tiltakozik ez ellen. Természetesen a kívánságát figyelembe kell venni. Az Avtv. 3. § (2) bekezdése szerint, különleges személyes adat akkor kezelhető, ha azt egy törvény kötelezően elrendeli, vagy az érintett ehhez írásban hozzájárul. Tehát a kutatásba történő bevonás feltétele nem csak az, hogy az érintettet tájékoztassák, hanem az is, hogy a beleegyezését írásban adja meg. Más országok adatvédelmi törvényei nem ennyire szigorúak, ezért megengedik a szóbeli hozzájárulást is. Amennyiben a kutatási célokról nem adnak felvilágosítást, és így a páciens nem egyezik bele, akkor a kutatási célú felhasználás jogellenesé válik.

A fenti általános kutatási célú felhasználás egy nem meghatározott ideig érvényes, korlátlan engedély, amely az Avtv. szerint a belső adatvédelmi felelősnél tett nyilatkozattal bármikor visszavonható. Azt, hogy a kutatáshoz történő adatgyűjtésnek hogyan kell lefolyni, az Eüaktv. 21. §-a szabályozza. E paragrafus alapján a kutatáshoz igényelt adatokat az intézetvezetőtől vagy a belső adatvédelmi felelőstől írásban kell kérni. Az írásbeli kérelemben meg kell adni az adatkérés célját, az igénylő adatait, az adatok fajtáit. Az intézetvezető vagy az adatvédelmi felelős dönt arról, hogy az adatok kiadhatók-e, és ha igen, akkor ez hogyan történjen. Amennyiben a betegkartonok adataiból kigyűjtött információ nem személyes adat, akkor a korábban adott általános beleegyezés az adatok kiadásához elegendő. Mivel az adatok nem határoznak meg egy konkrét személyt, így a személyiségi jogok nem sérülnek. Természetesen a kutatók az eredeti betegkartonok adatait nem ismer-

[50] Az ismertetésre kerülő megállapítások bővített formában megjelentek: Dr. Alexin Zoltán: Személyiségvédelem az orvosi kutatásban, Lege Artis Medicinae, Vol. 16. No. 6., pp. 594-597 (2006).

hetik meg, az adatok kiválogatását a kutatók költségére, az adott intézmény adatvédelmi szabályzatában szabályozott módon, erre feljogosított adatkezelő (intézményvezető, kezelőorvos, vagy belső adatvédelmi felelős) gyűjtheti ki. Speciális eset az, amikor a kezelőorvos egyben az adatokat igénylő kutató. Az Európa Tanács és a Miniszterek Tanácsa R 97 (5) számú ajánlása 12.3. cikkelye kimondja, hogy a kezelőorvosoknak joguk kell legyen ahhoz, hogy az általuk kezelt páciensek adatait kutatásra felhasználják, amennyiben azok nem kívántak élni a kimaradás jogával. A kezelőorvos jogosult adatkezelő, aki az eredeti kartonokból kigyűjthet kutatási adatokat, azonban csak olyanokat, amelyek nem minősülnek személyes adatnak. A kutatási felhasználás továbbra is az Eüaktv. 21. §-ban szabályozott módon kell történjen, az intézetvezetőnek kell ehhez az engedélyt megadni.

Ha a kutatók által igényelt, gyűjtött egészségügyi adatok személyes adatok, akkor azok csak úgy adhatók ki a kutatóknak még a saját kezelőorvosnak is, ha ehhez az érintett írásban hozzájárult. Ebben az esetben speciális, az adott alkalomra szóló, az adott felhasználásra vonatkozó írásbeli engedély szükséges, amelyet ehhez mért, adekvát tájékoztatásnak is meg kell előzni. Az engedély utólag is beszerezhető, mivel a páciens lakcíme, telefonszáma kiadható a kutatóknak ebből a célból (ha ezt korábban nem tiltotta meg, azaz nem kívánt élni a kimaradás jogával). Adott esetben ez egy járható út. Ha a kutatáshoz valóban szükségesek a személyes adatok, akkor azok felhasználására a pácienstől lehet és kell is engedélyt kérni. Ugyanez az eljárás található Elizabeth France adatkezelési útmutatójában[51], és ez összhangban áll az EGE (European Group on Ethics in Science and New Technologies Group) etikai ajánlásaival is.[52] Az Avtv. 3. § (2) bekezdése szerint különleges adat akkor kezelhető, ha ehhez az érintett írásban hozzájárul. Ha az adatkezelés egyéb törvényes feltételei fennállnak, akkor a felvilágosítás után adott önkéntes beleegyezés (informed consent) alapján az adatok kezelhetők. Egyes esetben bizonyos kutatások esetén egy törvény elrendelheti személyes egészségügyi adatok gyűjtését, azonban ennek a törvénynek nagyon komoly intézkedéseket kell tartalmaznia az érintettek magánéletének védelme érdekében.

8.2. Az orvosi kutatások etikai feltételei

Ebben a fejezetben azt mutatjuk be, hogy amennyiben az adatvédelmi törvényt elfelejtenénk, és csupán a jelenleg érvényes etikai szabályok alapján járnánk el, akkor is ugyanezt a kívánatos eljárást kapjuk. Tehát az adatvédelmi törvény nem enyhébb és nem szigorúbb, mint az orvosi szakma alapvető etikai szabályai. Akármelyik szerint is járnak el a kutatók, ugyanazt kell tenniük.

Az Orvosok Világszövetsége 1949-ben fogadta el az ún. Genfi Nyilatkozatot, amely a ma diplomázó orvosok esküje. Ez helyettesíti az ókorból származó Hippokratészi esküt. Az eskü szövegében szerepel, hogy az orvos a páciens által elmondott titkot még a halál után is megőrzi, senkinek sem adja tovább. Ez a kívánalom megjelenik az Eüaktv. 8. §-ában is mint kötelező törvényi előírás. Ebből az következik, hogy az orvos, ha esküjéhez hű kíván maradni, akkor a páciens gyógykezelése céljából az adatokat egy másik orvosnak csak a páciens kérésére (esetleg vélelmezett kérésére) adhat át. Orvosi kutatási célból, pedig csak kifejezett felhatalmazás birtokában. Ezt a rendkívül súlyos erkölcsi kötelességet egy in-

[51] Use and Disclosure of Health Data
[52] Ethical Issues of Healthcare in the Information Society, 10. oldal, 2.3. pont (1999).

tézmény sem hághatja át úgy, hogy az intézményvezető, vagy a kezelőorvos és főleg a páciens tudta nélkül a számítógépbe rögzített adatokat a kutatók egyszerűen megszerzik.

A II. világháború után ugyancsak az Orvosok Világszövetsége dolgozta ki az emberen végzett orvosi kutatások végzésének minimális etikai kívánalmait, amelyek Nürnbergi törvények (Nuremberg Code)[53] néven váltak közismertté. Ez volt a jogalapja a kísérletező náci orvosok elítélésének. A legfontosabb kinyilvánított etikai alapelv az önkéntesség volt. Orvosi kutatás csak önkéntes beleegyezéssel végezhető. Ha ennek az analógját keressük az adatvédelmi törvényben, akkor az önkéntességnek a kimaradás joga felel meg. Vagyis bárki, aki egy gyógyintézetet felkeres, ahol a gyógyítás mellett orvosi kutatást is folytatnak, élhet a kutatásból történő kimaradás jogával (ami miatt semmilyen hátrány nem érheti stb.). A Nürnbergi törvények szolgáltak alapul a Helsinki Nyilatkozathoz, amelyet azonban csak hosszas előkészítő munka után végül 1964-ben Helsinkiben fogadtak el.

A Helsinki Nyilatkozatot azóta már többször módosították. Azonban hosszú évek óta változatlan etikai alapelv, egy etikai kontrol beépítése, egy engedélyező, jóváhagyó intézményé, a kutatásetikai bizottságé. Minden orvosi kutatást egy etikai bizottságnak kell elbírálni, jóváhagyni. Az etikai bizottság fontos alapkérdéseket vizsgál például azt, hogy egyáltalán szükséges-e a kutatást emberen végezni, alkalmas-e a választott kutatási módszer, protokoll a kívánt cél elérésére, valóban várhatók-e azok az eredmények, amelyeket a javaslattevők állítanak, nem sérül-e a páciensek valamilyen érdeke, nem jár-e aránytalan egészségi kockázattal a végzett kutatás stb. Ha a kutatás valamilyen szempontból kétséges, akkor az engedélyt nem adják meg.

A fenti szigorú feltételek kinyilvánítása után már csak az a kérdés maradt nyitva, hogy vajon mi az orvosi kutatás definíciója. Adatvédelmi szempontból természetesen az a kérdés érdekes, hogy vajon a betegkartonok feldolgozása kutatás-e. Az nyilvánvaló, hogy pusztán az adatkezelés a páciens egészségét nem veszélyezteti, nem jár invazív beavatkozással. Mindazonáltal súlyos etikai problémát vet fel, nevezetesen azt, hogy akkor meg lehet-e a fentebb felsorolt szigorú előfeltételeket kerülni azzal, hogy mindazokat a vizsgálatokat és interjúkat a kutatók a gyógykezelés során elvégzik, amelyek a kutatáshoz szükségesek, azonban ehhez a szükséges engedélyeket nem szerzik be sem az etikai bizottságtól, sem a pácienstől. A folyamatot gyógykezelésnek állítják be, sok esetben nem is alaptalanul, hiszen közben megtörténik a gyógykezelés is. Ezt felismerve az Orvosok Világszövetsége 2000-ben Edinburghben egy olyan változtatást fogadott el, amely a Helsinki Nyilatkozatot megfelelően módosította. A módosítás lényege, és ezt mindjárt a nyilatkozat első pontjában kinyilvánítják, hogy az azonosítható személyek egészségügyi adatainak feldolgozása is orvosi kutatás. Ez volt az az erkölcsi zárókő, amely szükséges volt ahhoz, hogy teljessé váljon az etikai rendszer és megvalósuljon az adatvédelmi szabályokkal való teljes kompatibilitás. Ennek a következtében ugyanis a továbbiakban nem lehet megkerülni adatbázis-feldolgozás esetén sem az etikai bizottsági engedély megszerzését. Az etikai bizottság engedélyéhez csak akkor juthatnak hozzá a kutatók, ha biztosítják a résztvevők önkéntességét, az írásos beleegyezés lehetőségét, az előzetes felvilágosítást.

Arra is van mód, hogy a kutatást az etikai bizottság, illetve az adatvédelmi felelősök úgy engedélyezzék, hogy ne kelljen minden egyes pácienstől külön-külön írásbeli engedélyt beszerezni. Erre az adatvédelmi törvény akkor nyújt lehetőséget, ha az engedély beszerzése túlságosan nagy erőfeszítéssel járna, mert például sok pácienst kellene értesíteni. Ilyen esetekben, országos napilapokban, televízióban kellene a kötelező, előzetes felvilá-

[53] A Wikipédián: http://en.wikipedia.org/wiki/Nuremberg_Code

gosítást megtenni és felajánlani a kimaradás jogát. Az eredeti betegkartonokról csak nem személyes adatok gyűjthetők, és csak olyan páciensek adatai dolgozhatók fel, akik nem kívántak élni a kimaradás jogával.

Az is lehetséges, hogy egyes betegségek országos adatbázisába, ha azt egy törvény kötelezően elrendeli, a páciens beleegyezése nélkül lehessen adatokat továbbítani kutatási célból. Amennyiben egy megbetegedés a társadalom tagjaira veszélyt jelent (pl. fertőző betegség), akkor a páciensnek fel kell fednie személyazonosító adatait, erre törvény kötelezi. Az így a betegellátó tudomására jutott adatokat lehet az országos adatbázisba továbbítani. Ha a személyazonosság felfedése nem kötelező, akkor az adattovábbítás csak akkor lehetséges, ha a páciens önként ehhez hozzájárult. Nyilvánvalóan, az országos adatbázisban tárolt adatokon végrehajtandó kutatáshoz is szükség van az etikai bizottság támogató véleményére.

Ellenőrző kérdések

1. Milyen könnyítéseket, privilégiumokat élvez a tudományos kutatás a 95/46/EK irányelv szerint?

2. Milyen korlátozások érvényesek a levéltári kutatásokra, személyes adatok kutatása esetén?

3. Miként értelmezte az adatkezelés tisztességességének követelményét Elizabeth France?

4. Miért jelentkezik jelentős társadalmi problémaként a személyes egészségügyi adatok kutatásának problémája?

5. Milyen adatvédelmi feltételei vannak a személyes adatok kutatási célú felhasználásának?

6. Mi a teendő, ha az érintettek már nem élnek, vagy a hozzájárulásuk megszerzése túlságosan nagy erőfeszítést jelentene?

7. Felhasználhatja-e kutatásra a kezelésében lévő személyes egészségügyi adatokat az érintettek kezelőorvosa?

8. Az Európa Tanács mely dokumentuma foglalkozik az egészségügyi adatok kezelésének elveivel?

9. Szabályozza-e törvény Magyarországon az orvosi titoktartást?

10. Mely szervezet dokumentuma az orvosi kutatásokat szabályozó Helsinki Nyilatkozat?

11. Mi volt a forrása annak a társadalmi igénynek, amely létrehívta a Helsinki Nyilatkozatot?

12. Mit mond az orvosi etika a személyes egészségügyi adatok kutatási felhasználásáról?

9. A biometrikus azonosítási módszerek

Biometrikus azonosítási módszereknek nevezzük azokat a módszereket, amelyek az egyes embereket jellegzetes egyéni, biológiai tulajdonságaik alapján azonosítja. Ennek a módszernek megfelelően specifikusnak, azaz nagyszámú ember között nagy biztonsággal kell azonosítania a kívánt személyt, viszonylag egyszerűen kivitelezhetőnek, és természetesen költséghatékonynak is kell lennie. A biometrikus azonosítási módszerek előnye, hogy az ember ezeket a jellemzőket nem veszíti el, mindig kéznél vannak, a felnőtteknél már nem változnak az életkor előre haladásával, esetenként még sok évvel a halál után is alkalmasak személyazonosításra. A magánélet szempontjából azonban ellentmondásos a szerepük, ugyanis az emberek így akaratukon kívül is azonosíthatóvá válnak, mozgásukat, tevékenységüket folyamatosan megfigyelés alatt lehet tartani, ráadásul mindezt anélkül, hogy az érintettek erről tudomást szereznének. Az emberek ezért óvatosan fogadják, és kissé idegenkednek az ilyen azonosítási módoktól.

Alapvetően három speciális terület látszik kialakulni e területen belül:

- Fiziológiai azonosítási módszerek
- DNS alapú módszerek
- Viselkedés alapú módszerek

A fiziológiai módszerek közé tartoznak az emberi test bizonyos méretei pl. tenyér és az ujjak mérete, geometriája, az arc formája és mérete, az ujjlenyomat, a tenyérlenyomat, a talplenyomat, ajaklenyomat foglenyomat jellegzetességei, de ide tartozik a bőr alatti erek mintázata, amelyet infrakamerával lehet láthatóvá tenni, ehhez nagyon hasonló a szem ideghártya ereinek rajzolata, vagy az írisz egyedi mintázatán alapuló felismerés.

Az ujjlenyomat személyazonosításra történő felhasználása a XIX. század végén indult meg. Ekkor fedezték fel, hogy az ujjak (tenyér, talp) jellegzetes rajzolata egyedi és az életkorral nem változik. Később osztályozási módszereket fejlesztettek ki, amelyek a rajzolat néhány jellegzetességét, alapstruktúráját ragadják meg. Az ujjlenyomat osztályozás birtokában nem kell egymásra helyezni és pixelenként összehasonlítani az ujjlenyomatokat, hanem a jellegzetes jegyek alapján, alakfelismerési módszerekkel meg lehet határozni néhány fontos jegyet (pl. ívet, örvényt, hurkot és ezek alosztályait), amelyekkel az azonosítás automatikusan elvégezhető. Ez kiküszöböli azt a problémát, amit az okoz, hogy az ujjat sosem pontosan azonos módon helyezik el a szenzoron. Ha több ujjról is rendelkezünk ujjlenyomattal, akkor egy-egy ujjról kevesebb alaki jegy is elég az azonosításhoz.

Az ujjlenyomat leolvasó elektronikus szenzorok lehetnek mátrix elven működők, amelyek egyetlen művelettel leolvassák a ráhelyezett ujj képét. Vannak soros leolvasó eszközök is, amelyeket főként laptopokba beépítve használnak. Ezek előtt fokozatosan lefelé kell mozgatni az ujjat, és soronként olvassa le az ujjlenyomatot. A jelenlegi érzékelők és a hozzájuk tartozó szoftver még nem elég pontos, ami azt jelenti, hogy elég gyakran hibáznak. A szenzor működését befolyásolja, a nyomóerő, az ujj elhelyezkedése, esetleges remegés, a hőmérséklet.

Az ujjlenyomat nagyon kis mennyiségben tartalmazhat bőrsejteket, illetve az ujjról leváló kémiai anyagokat, amely segíthet egy személy azonosításában. A modern technika lehetővé teszi azt, hogy az ujjlenyomatban talált néhány sejt DNS-ét enzimekkel fel lehessen erősíteni (sokszorosítani), majd pedig DNS alapú azonosítást lehessen végezni. Az

ujjlenyomatban szereplő kémiai anyagok azonosításával az érintett személy szokásaira, foglalkozására, utoljára végzett tevékenységére lehet következtetni. Ki lehet mutatni ezen a módon kábítószereket, oldószereket, nikotint, festékeket. Az ujjlenyomatot a DNS tartalma miatt az Európai Bizottság jelenleg különleges személyes adatnak tartja. Ez akadályozza a vállalati ujjlenyomat alapú beléptető rendszerek elterjedését.

Az ujjlenyomat nem egyedi minden egyes személyre, hiszen az egypetéjű ikrek esetén az ujjlenyomat azonos, az esetek 0,2%-ában, azaz kb. minden ötszázadik embernél. Az írisz kép azonban minden egyes személy esetén egyedi, a bal és a jobb szem mintázata is szignifikánsan különböző, és az élet során nem változik az eddigi vizsgálatok szerint. Még a genetikailag azonos ikrek esetén is különbözik az írisz képe. Míg az ujjlenyomat egyes foglalkozások esetén rongálódik, erodálódik, addig az írisz kép jól védett, nehezen sérül meg. A pupillától kifelé sugárirányban terjedő részletgazdag struktúra. Megfelelő kamerával 10 cm távolságról érintkezés nélkül lehet róla képet készíteni. Az azonosítást ugyanakkor befolyásolhatja a szemre felhelyezett pl. színes vagy mintás kontaktlencse.

Az írisz mintázatának felismerésére John Daugman[54] dolgozott ki egy sikeres algoritmust. Ez előbb két koncentrikus kört és a szemhéjat különíti el, amelyek között helyezkedik el a felismerendő terület, majd erre a veszteséges tömörítő algoritmusokhoz hasonló, a spektrális komponenseket meghatározó transzformációt alkalmaznak. Ennek végén egy 2048 bit hosszúságú jelzőszámot kapnak. Két írisz kép közötti hasonlóságot a Hamming távolsággal számítják ki, ami jelen esetben a különböző bitek számát jelenti. Az Egyesült Arab Emirátusban a jelentős számú illegális bevándorló kiszűrésére vezettek be egy kísérleti rendszert. A női viselet itt gyakran a csador, ami akadályozta az útlevél tulajdonosának megbízható azonosítását. Minden beérkező külföldiről írisz képet vettek fel. Néhány év alatt egy 630 ezer személy írisz képét tartalmazó adatbázist kaptak. Ezután megvizsgálták a különböző írisz képek távolságának eloszlását. A kapott eredmények alapján egy olyan távolság küszöbértéket határoztak meg, amely minden különböző írisz képet el tudott különíteni, az egyezőket pedig elfogadta. Végül a mintegy 200 milliárd összehasonlítás során a rendszer egyetlen hibát sem vétett. Az Egyesült Királyságban, Hollandiában, az Egyesült Államokban és Kanadában működik írisz kép alapú, kísérleti határátlépési rendszer. A regisztrált utazóknak egy kamerába kell nézni, majd zöld jelzés esetén további azonosítás nélkül léphetnek be az országba.

A kutatók megpróbálták módszerüket emberi arc felismerésére alkalmazni. Ennek a sikeressége azonban messze elmaradt az írisz kép felismeréstől. Nagyszámú összehasonlításkor komoly mértékben, akár 20-30%-ban is hibázott az algoritmus. Az arcfelismerés sikertelenségét befolyásolja a haj, az mimika, az arc síkja, a megvilágítás, sminkelés.

A DNS alapú módszerek az emberi örökítő anyag jellegzetességei alapján azonosítják az egyes személyeket. Ehhez bármilyen kicsiny mennyiségű biológiai minta, testnedv, (bőr)szövetdarab elegendő. A kutatók több mint száz olyan speciális genetikai helyet (markert) találtak a kromoszómákon, amelyek nagy diverzitást mutatnak, azaz az emberek rendkívül sokfélék, ha ezeket a helyeket genetikai módszerekkel vizsgálják. Ha 10-20 ilyen pozíciót tekintünk egy adott személynél, akkor egy olyan érzékeny módszert kapunk, ami nagy valószínűséggel kiválasztja őt a világon élő összes más ember közül. A genetikai módszerek alkalmasak származási kapcsolatok felderítésére is. Egypetéjű ikrek esetén azonban az ikerpárokat nem tudja megkülönböztetni. A genetikai vizsgálat eredménye: a

[54] John Daugman professzor, University of Cambridge, honlapja: http://www.cl.cam.ac.uk/~jgd1000

marker pozíción található változatok (allélek) sorozata. Ez az adott személyt már egyedileg azonosítja, ezért genetikai ujjlenyomatnak (genetic fingerprint) is nevezik.

Alec Jeffreys 1984-ben fedezte fel ezt a lehetőséget, amikor ismétlődő, de fehérjét nem kódoló, azonban egyénileg változó szekvenciákat talált az emberi génekben. Első törvényszéki alkalmazásukra 1986-ban került sor. A genetikai ujjlenyomatot egy hash függvénynek is tekinthetjük, mert az öröklődő genetikai tulajdonságokból nem fed fel egyet sem, mégis megkülönbözteti az egyes embereket egymástól. A bűnügyek helyszínein gyakran marad hajszál, nyál, váladék, vér vagy bőrsejt. Az ezekből kivont DNS ujjlenyomat azonosíthatja a tettest vagy az áldozatot. Az egyes államokban törvény szabályozza a súlyos erőszakos bűncselekmények elkövetőinek DNS mintavételét, bűnmegelőzés céljából. Ezeket a mintákat egy nemzeti adatbázisban tárolják. Magyarországon a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény szabályozza a bűnügyi célú DNS ujjlenyomatok kezelését. Az idők során tekintélyes méretű adatbázis jött létre. Az Egyesült Királyságban már 600 ezer mintát őriznek. Az EJEB nemrégen egy magánszemély indítványára elmarasztalta az Egyesült Királyságot, mivel az adatbázisban együtt szerepeltették a tanúk és sértettek DNS mintáit az elkövetőkével, továbbá a vétlen személyek mintáit nem semmisítették meg. Az Egyesült Királyságban merült fel az a kérdés, hogy orvosi kutatásokra fel lehetne-e használni a bűnügyi mintákat – erre az Európai Bizottság *nem* választ adott. Az is felmerült, hogy a rossz iskolai magaviseletű gyerekektől is DNS mintát kellene venni, azonban végül ezt az ötletet is elvetették.

Az MTA Szegedi Biológiai Kutató Intézetében[55] (SzBK) Dr. Raskó István genetikus professzor foglalkozott az Árpád kori csontmaradványok genetikai ujjlenyomatának vizsgálatával. Egyrészt az anyai ágon öröklődő mitokondriális DNS gyűrű egy speciális régióját vizsgálta, illetve az apai ágon öröklődő Y kromoszóma nemkódoló régióit. Az ujjlenyomatok alapján családi kapcsolatokat, eredetre utaló genetikai tulajdonságokat kerestek és találtak. Felfedezték az úgynevezett genetika órát, amely történelmi viszonylatban jellemzi a genetikai mutációk megjelenési sebességét. Az IBM támogatta azt a másik világméretű kutatást, amely az egész világon térképezte fel a lakosság jellegzetes népcsoportjainak genetikai ujjlenyomatát. Az utóbbi időben felmerült az a lehetőség, hogy laboratóriumban szintetizált genetikai ujjlenyomatot lehet előállítani, amivel tévútra lehet vezetni egy nyomozást.

A viselkedés alapú azonosítás egyik példája az aláírás azonosítása, de vannak már a billentyűzeten gépelés jellegzetességein, hangfelismerésen, a járás jellegzetességein alapuló azonosító eljárások. Az aláírás az évek során jellegzetessé válik. Ezért számos esetben használják biometrikus azonosításra, például pénzintézetekben. Az aláírásnál nem lehet egyszerűen a képeket egymásra helyezni, hanem inkább az írás vonalvezetésének jellegzetességeit kell meghatározni. A grafológia egy olyan szakma, amely az írás morfológiai jegyeit összegyűjtötte. Ezeket a jegyeket számítógépes alakfelismerési módszerekkel is lehet detektálni. Két aláírás egyezőségének megállapítása egyszerűbb feladat, mint általában a kézírás átalakítása szöveges állománnyá. Utóbbi esetben az egyes leírt és esetleg elnagyolt karaktereket is egyenként fel kell ismerni.

A számítógépek sebessége elegendően nagy ahhoz, hogy a billentyűzeten az egymás után lenyomott betűk közötti időtartamokat pontosan le lehessen mérni. A gépelési sebes-

[55] Honlapja: http://www.szbk.hu/

ség, jellegzetességei is hordoznak személyre jellemző információt, amelyet személyazonosításra fel lehet használni. Ilyen programok már készültek, hozzáférhetők a felhasználók számára.

Az emberi beszélő felismerése a hang spektrális összetevőinek elemzésével és összehasonlításával végezhető el. A hangszín jellegzetességeit a hangképző szervek mérete, alakja, és az üregek falának rugalmassága befolyásolja. Ezek a tényezők a spektrális összetevőkre is hatnak. Összehasonlításkor számításba jöhet még a háttérzaj, az elektronikus rendszer frekvencia átviteli karakterisztikája is. Megkülönböztetnek fix szövegű és kötetlen szövegű eseteket. Az első esetben egy jelszót, vagy mondatot kell a beszélőnek bemondania, és a rendszer ez alapján ismeri fel. A beszéd statisztikai jellemzői miatt a HMM (Hidden Markov Model, Rejtett Markov modell) alapú eljárások sikeresen alkalmazhatók erre a célra. Rontja a felismerést, ha az érintett bereked, megfázik, kihúzták a fogát stb.

A beszéd jellegzetességeit fel lehet használni arra is, hogy a beszélő lelki állapotát, izgatottságát, pszichológiai tulajdonságait detektálják. Kísérleti szoftverek készültek már abból a célból, hogy telefonos vevőszolgálatok hívóinak izgatott állapotát automatikusan detektálják (a rögzítésre kerülő telefonhívások feldolgozásával). A szoftver által jelzett esetekben azután egy munkahelyi vezető beavatkozhat, és jó irányba terelheti a reklamáció további megoldását.

Ellenőrző kérdések

1. Milyen főbb csoportokra oszthatók a biometrikus azonosítási módszerek?
2. Milyen előnyei és hátrányai vannak a biometrikus azonosításnak?
3. Mi az alapja az ujjlenyomat alapú azonosítási módszernek?
4. Hogyan lehet nagyméretű ujjlenyomat adatbázisban hatékonyan keresni?
5. Vannak-e olyan esetek, amikor korlátozottan működik az ujjlenyomat alapú azonosítás?
6. Az írisz kép alapján történő azonosításnak mik az előnyei és mi ennek a biológiai alapja?
7. Hogyan és mely törvény alapján működnek a bűnügyi ujjlenyomat, illetve DNS adatbázisok?
8. Ki és mikor fedezte fel a genetikus ujjlenyomatot?
9. Mi a genetikus ujjlenyomat biológiai alapja.
10. Milyen viselkedés alapú biometrikus azonosítási módokat ismer?

10. Az elektronikus kommunikáció adatvédelmének egyes kérdései

Az elektronikus hálózatokon nemcsak jóhiszemű felhasználókat találunk. Néhányan a hálózatokat ártó szándékkal használják, rombolnak, másokat megfigyelnek, szolgáltatásokat lehetetlenítenek el. Az elkövetők a hálózati számítógépek védelmi hiányosságait használják ki. Kezdetben csak a védelem kijátszásának ténye volt érdekes, valójában egy ártatlan programot (adatállományt) juttattak be egy gyanútlan másik felhasználó számítógépére. Az analógia alapján az ilyen szoftvereket számítógép vírusoknak nevezték el. A számítógép vírusok is tudtunkon kívül kerülnek rá a számítógépünkre, ellenőrizhetetlen módon másolják át magukat egy újabb gépre, gyengítik az operációs rendszer védekezőképességét és munkabírását mivel erőforrásokat foglalnak le, kötnek le. A számítógép vírusok később specializálódtak, illetve más-más módon próbálták meg a hálózatok rendeltetésszerű működését akadályozni. Ennek megfelelően manapság olyan szoftvereket is vírusnak nevezünk, amelyek nem a klasszikus módon működnek, de tudtunkon kívül a számítógépünkre kerülve befolyásolják annak működését, ezért az utóbbi időben malware, malicious software elnevezést is használják rájuk. A Magyar Köztársaságban a számítógéprendszerekbe történő behatolás, károkozás, illetve a működés megzavarása vétség vagy bűncselekmény. A büntető törvénykönyvről szóló 1978. évi IV. törvény 300/C. és 300/E. szakaszai szólnak ezekről.

> 300/C. § (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.
>
> (2) Aki
> a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl, vagy hozzáférhetetlenné tesz,
> b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.
>
> (3) Aki jogtalan haszonszerzés végett
>
> a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy
> b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,
> és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.
>
> (4) A (3) bekezdésben meghatározott bűncselekmény büntetése
> a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,
> b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,

> c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.
>
> 300/E. § (1) Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot
>
> a) készít,
> b) megszerez,
> c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz,
>
> vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.
> (2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.
> (3) Nem büntethető az (1) bekezdés a) pontja esetén, aki – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

Az eleinte ártalmatlan vírusok célja kezdetben csak a saját sokszorosításuk volt, illetve a felhasználók bosszantása. Ezzel egy időben azonban a durva károkozás is lehetővé vált, például értékes fájlok törlése, mágneslemez formázás, valamely szolgáltatás blokkolása. A titokban a számítógépen tevékenykedő és szaporodó vírusokat férgeknek nevezik, angolul worm. A programok másik csoportja a gyanútlan számítógépek kikémlelését, az irányítás megszerzését tűzte ki célul. Ezeket kémprogramoknak spyware-nek hívják. A kémprogram közvetítheti a video memóriát (az aktuális felhasználó képernyőjét), a billentyű leütések sorozatát a megfigyelőnek. Lehetővé teheti különböző parancsok távoli futtatását, adott esetben rendszergazdai jogokat is képes megszerezni a fertőzött számítógépen – mindezeket titokban. Egy újabb vírus típus a trójai faló, amit hátsó ajtónak (backdoor) is neveznek, arra szolgál, hogy később tetszés szerinti időpillanatban rajta keresztül újabb kártékony szoftvereket lehessen a megtámadott számítógépre telepíteni. Így a számítógép feletti ellenőrzést megszerezhetik, de ennek a lehetőségnek a kihasználását nem azonnal kezdik meg. A trójai falovak mindazonáltal alkalmasak arra, hogy az érvényes jelszavakat, esetleg rendszer szintű állományokat, konfigurációkat közvetítsenek a számítógépünkről illetéktelenek számára.

A számítógéprendszerek működésének megzavarása egy olyan újabb találmány, amit a trójai falovak tettek lehetővé. A DOS (Denial Of Service, kiszolgálás megtagadása) egy olyan incidens, amelynek során számos kliens egyszerre jelentkezik kiszolgálási igénnyel és ez lehetetlenné teszi a szolgáltatás normál működését. Tipikusan egy-egy web portálra befutó nagyszámú kérést jelent, mondjuk egy választási eredmény, időjárás, online folyóirat esetén. A DOS kivitelezéséhez időzített támadásra van szükség, amelyet nem egyetlen gépről hajtanak végre, hanem a világban szétszórt több ezer számítógépről, természetesen a gazdáik tudomása nélkül. Ennek megszervezésére a trójai faló vírusok alkalmasak.

A számítógép hálózatokon elküldött kéretlen levelek (spam), lassítják a normál levelezés folyamatát, és a felhasználók idejét is rabolják – hiszen ki kell őket törölni, illetve el kell őket olvasni törlés előtt. Az egyes országok megpróbálják jogellenessé tenni az ilyen levelek küldését azonban nem túl sok sikerrel. Egy felmérés szerint a levelek háromnegyede jelenleg kéretlen reklámlevél. A levelek a bosszankodáson túl konkrét károkat is okozhatnak – gondoljunk a különböző nyereményekről értesítő levelekre. Itt nyereményről szó sincs, a közvetítési díjat beszedik a bűnözők, majd eltűnnek a pénzzel. Mások értéktelen, hamisított árukat kínálnak a gyanútlan felhasználóknak.

A tapasztalatlan web felhasználók életét keserítik meg az adathalász web alkalmazások. Ezek azt használják ki, hogy megtévesztett emberek egy ismert szolgáltatónak gyanakvás nélkül megadják az adataikat, például egy banknak. Az adathalászok az eredeti banki weboldalt lemásolják és egy megtévesztésig hasonló webcímre telepítik. Ezután, kéretlen levelet küldenek ki nagyszámú felhasználónak, hogy jelentkezzenek be a bank oldalára, a megadott linkre kattintva. A gyanútlan felhasználók pedig megadják a bankszámlaszámukat, belépési azonosítójukat, sőt még a jelszavukat is a bűnözőknek. Vannak olyan weboldalak, amelyek ismert vagy jól hangzó nevű szoftvereket kínálnak letöltésre, azonban letöltéskor a felhasználók egy adathalász programot, vagy egy vírust telepítenek a gépükre. Számos Internet Explorer toolbar programról derült ki, hogy egy féreg, mivel egy alapfunkcióval leplezve, adatokat továbbít, hirdetéseket, szoftvereket tölt le a számítógépekre kéretlenül a tulajdonos tudta nélkül.

A vírusok számos módon, rendkívül találékonyan leplezik a működésüket. Először is elrejtik a kódjukat. Olyan mágneslemez területeket használnak fel, amelyek nem elérhetők a normál felhasználók számára. Vannak partíciós táblába, vagy boot rekordba épülő vírusok. Mivel itt a memória terület kicsi, ezért a vírus nem tud komolyabb feladatokat ellátni. A mágneslemezen azonban a 0. sávon a fájl allokációs tábla előtt vannak még nem használt területek, a vírusok ide is beépülhetnek. Gyakran meglévő, az operációs rendszerben szokásosan használt fájlneveket használnak, ezért nem tűnik fel, hogy a szokásos program helyébe lépett a vírus. Több esetben a vírus ellátja azokat a tevékenységeket, amelyet az eredeti program is ellátott, ezért a tevékenysége még inkább rejtve marad. A vírusok más esetben a memóriában vannak folyamatosan és rendszerleálláskor újból a mágneslemezre íródnak. Így hiába távolítják őket el az egységekről, ismét visszakerülnek. A vírusok működésüket sokszor elrejtik, például nem publikált gépi utasításokat használnak, ezért a szokásos disassembler programok nem tudják kilistázni a kódot. Máskor enkriptált kódrészleteket használnak, és előbb vissza kell kódolni őket a megfejtéshez.

A vírusok elleni védekezés vírusirtó programok telepítésével valósítható meg. Számos ismert program áll rendelkezésre: Ad-Aware, Norton Antivirus, NOD32 stb. A vírusirtó programokhoz rendszeres frissítés is tartozik. Az egyre újabb vírusokat a gyártó cégek folyamatosan figyelik és felderítik a működésüket. Ezután kidolgozzák az eltávolítás, blokkolás módját, majd tesztelik és frissítik a vírusirtó programokat ezzel az új képességgel.

A vírusok készítői rendszerint az elterjedt operációs rendszerek fogyatékosságait használják ki. Mivel a számítógépek jelentős részén Windows operációs rendszer fut, ezért természetesen erre készítik a vírusok legnagyobb részét. Manapság a nagyobb szerverparkok működtető szoftvere is valamilyen Windows szerver operációs rendszer, ezért a más Windows rendszerekben megszerzett tudást, a víruskészítők felhasználják a szerver operációs rendszerek elleni támadásra. Amennyiben fontos vállalti, kormányzati feladatokat Windows szerver operációs rendszert futtató számítógépekkel valósítanak meg, akkor gon-

dolni kell a vírusveszélyre. Mivel a futtatott szoftverek rendkívül változatosak, és a bonyolult operációs rendszer sem tud ellenállni minden támadásnak, ezért igény mutatkozik az ún. etikus hackerekre, akik vállalati megbízást kapnak arra, hogy a telepített rendszerek gyenge pontjaira rátaláljanak. Amikor egy hátsó bejáratot találnak, akkor azt természetesen gyorsan lezárják. Az etikus hackerek éves konferenciáját Hacktivity-nek[56] nevezik, évente Budapesten rendezik meg.

Ellenőrző kérdések

1. Milyen károkat okozhatnak a számítógép vírusok?
2. Büntetőjogilag felelősségre lehet-e vonni egy vírus készítőjét?
3. Milyen bűncselekményeket lehet elkövetni egy számítástechnikai rendszerrel szemben?
4. Mit jelent a spyware kifejezés?
5. Mik a trójai falovak?
6. Mi a DOS támadás alapja, és hogyan szervezik meg?
7. Hogyan tudnak eltűnni szem elől a számítógépes vírusok?
8. Mely operációs rendszerek vannak leginkább kitéve vírusok támadásának?
9. Mi az adathalászat?
10. Hogyan lehet személyes adatokhoz jutni az adathalászat módszerével?

[56] A konferencia honlapja: http://www.hacktivity.hu

11. A fizikai adatvédelem

Az Avtv. 10. §-a kötelezi az adatkezelőket arra, hogy a kezelésükben lévő személyes adatokat biztonságos körülmények között tárolják. Ennek érdekében technikai és szervezési intézkedéseket kell tenniük.

> 10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
>
> (2) Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

A számítástechnikai rendszerek fizikai adatvédelmével több szabvány is foglalkozik, amelyeknek történő megfelelést akkreditáló szervezetek vizsgálják, és erről tanúsítványokat állítanak ki. Ilyen szabványok például a nemzetközi ISO 27001 (Information Security Management, információs biztonság menedzsment), vagy az ISO 22857 (Health Informatics, egészségügyi informatika) szabvány.[57] E szabványok mögött nemzetközi munkacsoportok vannak, amelyek a szabványokat karban tartják, időnként újabb verziókat bocsátanak ki. A verziókat a kibocsátás évével jelölik pl. ISO 27001:2004. Az ISO 27001 ismeretek magyarországi terjesztésében, oktatásában jelentős szerepet tölt be a Hétpecsét Egyesület[58]. A szabványokban instrukciók vannak arra, hogy egy adott vállalatnál hogyan és milyen szervezési intézkedéseket kell hozni az adatbiztonság érdekében.

Az információbiztonsági szabvány lényege, hogy az informatikai tevékenységek, eszközök, kapacitások, személyi felelősségek, hatáskörök, továbbfejlesztések, kockázatok felmérése történjen meg, legyen írásba foglalva, és a vezetés ennek tudatában hozzon meg minden döntést, ami az információfeldolgozással kapcsolatos.

- a vezetésnek bizonyítani kell elkötelezettségét az információbiztonság iránt, amelynek pl. egyik megnyilvánulása, hogy meghatározza a kapcsolódó felelősség- és hatásköröket;
- az információbiztonság egy többszereplős feladat, amelybe a szervezet különböző részlegeinek megfelelő módon való képviselete szükséges;
- az új eszközök használatának engedélyezése és a védelemmel kapcsolatos titoktartási megállapodások megkötése is belső szervezeti kérdés;

[57] A svájci székhelyű ISO (International Standards Organization, Nemzetközi Szabványügyi Szervezet) honlapja: http://www.iso.ch
[58] http://www.hetpecset.hu

- fontos kérdés az érintett partnerekkel, érdekelt felekkel, szakmai körökkel való kapcsolattartás is, ami részben biztosítja a kérdéskörben való tájékozódást és naprakészséget;
- az információvédelmi intézkedések megvalósulásának független átvizsgálása a rendszer működésének, jóságának egyik lehetséges ellenőrzési módja. Ez utóbbi nem feltétlenül a tanúsításra vonatkozik, de burkoltan beleértjük azt a vonatkozó szabványkövetelménybe.[59]

A szabványnak történő megfelelést minden évben auditor (tanúsító) cégekkel újra és újra meg kell vizsgáltatni és az auditor cég által talált fogyatékosságokat ki kell küszöbölni. Meg kell azonban jegyezni, hogy a vállalati adatbiztonság kérdését nem annyira az érintett személyek emberi jogai vetik fel, hanem sokkal inkább a vállalat gazdasági érdeke. A termelésre, a partnerekre, a piacra, és nyersanyagokra, a saját vállalat anyagi helyzetére vonatkozó adatok a további sikeres működés szempontjából kiemelkedően szenzitív adatok, amelyek semmilyen körülmények között nem kerülhetnek illetéktelen kezekbe, akár személyes adatok ezek, akár nem.

A vállalati adatvédelem az összegyűjtött adatvagyon sérthetetlenségét, integritását, használhatóságát és bizalmas kezelését lehetővé tevő technológiák és szervezési módszerek összessége. Az adatvédelmi törvény megkívánja, hogy a személyes adatokat ilyen védelem mellett tárolják – ugyanakkor a vállalatok e kötelezettségüket rendszerint saját maguk kiterjesztik a vállalat szempontjából fontos minden egyéb, nem személyes adatra is. Amennyiben egy szervezet eleget tesz és tanúsítványt szerez egy információbiztonsági szabványra nézve, az nem jelenti azt, hogy az egész adatvédelmi törvény előírásainak eleget tesz – a tanúsítás egyedül az adatvédelmi törvény 10. §-ának történő megfelelést támasztja alá.

A létesítmények elzárása, védelme és őrzése

Ahogyan a termelő gépeket, gyártó berendezéseket folyamatosan őrzik, úgy a számítástechnikai eszközparkot is fontosságának megfelelő védelemben kell részesíteni. Minél értékesebb maga a központi számítógép, a szerver park, illetve a rajtuk tárolt adat annál körültekintőbb megoldásokat kell alkalmazni. Az épületet, amelyben az értékes gépek találhatók célszerű minél biztonságosabbra építeni. Ebbe beletartozik a betörés és szabotázs elleni védelem, de az elemi károk, üzemzavar elleni védelem is.

A gépek közelébe jutást is célszerű korlátozni. Erre néhány speciális engedéllyel felruházott személyt elég felhatalmazni. A szervereket kiszolgáló személyzet jórészt távolról is el tudja végezni a feladatát. A belépési jogosultság ellenőrzését bízhatjuk vagyonőrökre, vagy valamilyen elektronikus rendszerre. Természetesen a belépések adatait a rendszernek naplóznia kell. A belépéseket és az épület környékét kamerás megfigyeléssel lehet biztosítani. Ez megelőzheti belső munkatársak ártó szándékú tevékenységét. A tűz ellen automatikus riasztó és oltóberendezést lehet telepíteni. Az ablaktöréseket (betörésnél vagy viharkár esetén) törésérzékelőkkel, a robbanást, földrengést ugyancsak megfelelő érzékelőkkel észlelhetjük. Áramszünet ellen a szokásos védelem az automatikusan induló generátor, amelynek elindulásához szükséges ideig (10-15 perc) akkumulátoros szünetmentes áram-

[59] ISO 27001:2005, A melléklet 6.1. pontja.

forrásokat használhatunk. Az épületet célszerű statikailag is szilárddá tenni. A legféltettebb számítóközpontokat hegyek gyomrában, vagy a föld mélyén helyezik el.

A szerverpark folyamatos kapcsolatát a kommunikációs hálózatok felé úgy biztosíthatjuk, ha legalább két független internet szolgáltató felé létesítünk megbízható összeköttetést, és a két kommunikációs csatorna folyamatosan rendelkezésünkre áll, a forgalom dinamikusan átterhelhető egyikről a másikra. A földi vezetékhálózat sérülékenységét tartalék vezeték nélküli adatátviteli lehetőségekkel célszerű kiegészíteni, akár műholdas adatátvitellel, azonban gondolni kell arra, hogy ezek sebezhetőbbek és könnyen lehallgathatók.

A számítástechnikai gépek, berendezések védelme

Az értékes elektronikus adatfeldolgozó berendezéseket vagy azok részegységeit, tartozékait, az adattároló eszközöket fizikailag is védeni kell az eltulajdonítástól, sérüléstől, meghibásodástól, megsemmisüléstől. A könnyen mozdítható és szállítható kisebb berendezéseket elzártan kell tartani. Ezeket személyi felelősséggel, írásban kell átadni és visszavenni. Az ilyen eszközök elveszését gyakori leltár ellenőrzéssel is meg lehet akadályozni. A hibás eszközöket amennyiben lehet célszerű megjavíttatni minél előbb. Az eszközöket tároló helyiségekbe a belépést és távozást célszerű korlátozni, illetve a bejáratot kamerával megfigyelni.[60]

A számítástechnikai eszközök érzékenyek lehetnek folyadékokra, erős napfényre, hőre, nagy nyomásra, erős mágneses terekre. Ezekre a használók figyelmét fel kell hívni és belső stratégiákat kell kidolgozni arra, hogy e nem kívánt hatásokat el lehessen kerülni. Az eszközök védelmére vonatkozó óvintézkedéseket már az épületek tervezésénél, épületgépészeti, vezetékezési terveknél figyelembe lehet venni. Az eszközök megbízható működéséhez szükséges, hogy a működtető szoftverek megbízhatók és üzemkészek legyenek. Ezért célszerű központi telepítéseket használni, előzetesen egy-egy telepítési konfigurációt tesztelni, és sikeres próba után kiterjeszteni a cég többi gépére. Az egyéni telepítéseket korlátozni célszerű, de legalábbis naplózni, figyelemmel kísérni.

Az adathordozók védelme

Az adathordozókat ugyanúgy, ahogyan a gépeket is, védeni kell az eltulajdonítástól, illetéktelen másolástól, leolvasástól. Teljes rendszerek, nagy adatbázisok biztonsági, mágnesszalagos vagy mágneslemezes mentésére ez fokozottan igaz. A fontos adatokat tartalmazó adathordozókat nyilvántartásba kell venni és őrzötten kell tárolni. Az adatszivárgás megelőzése érdekében a törlés, megsemmisítés is ellenőrzötten kell, hogy történjen. Mindig maradjon róla írásos feljegyzés (jegyzőkönyv). A nagyteljesítményű adatmentő, visszaállító, vagy másoló perifériák használatát korlátozni célszerű. A használatot és annak célját ugyancsak naplózni kell. Némely esetben sor kerülhet adathordozó elküldésére. Ekkor is megfelelő biztonsági intézkedéseket kell alkalmazni. A magyar adatvédelmi biztos állásfoglalása szerint kis mennyiségű normál személyes adatot közönséges postai küldeményben is lehet továbbítani. Nagyobb adatmennyiségnél, vagy különleges személyes adatok esetén azonban könyvelt (ajánlott, sőt tértivevényes ajánlott) küldeményt indokolt alkalmazni. Ennél is értékesebb szállítmány esetén futárszolgálatot lehet igénybe venni. A felbontás elleni védelem eszköze lehet a visszazárhatatlan (temper proof) csomagolás. Ilyenkor nem lehet észrevétlenül felbontani és visszazárni a csomagolást anélkül, hogy erre fény

[60] ISO 27001:2005, A melléklet 7.1. pontja.

ne derülne. Az adatok védelmét nagyban segíti, ha a szükségtelen adatokat a legrövidebb időn belül megsemmisítik. Esetenként a vállalatok gazdasági érdeke is megköveteli, hogy a törvényes megőrzési idő után a pénzügyi, adózási, társadalombiztosítási adatokat azonnal megsemmisítsék.

A kommunikációs hálózat védelme

Az elektronikus adatfeldolgozó berendezések hálózatát a hálózat felől érkező betörések, támadások és kémprogramok ellen is védeni kell. Ennek eszközei lehetnek a hálózati tűzfalak, privát hálózatok, hálózati forgalom szűrése és korlátozása. A hálózati kliensek egyedi azonosítása korábban a hálózati kártyák hardver címével történt, a MAC (Media Access Control) cím segítségével. Ezzel az azonosítóval jelentkeztek be a számítógépek, és ellenőrzés után ennek alapján kaphattak dinamikus IP számot, és kezdhettek forgalmazni a hálózaton. A modernebb hálózati kártyák esetén a MAC címet át lehet programozni, ezért a MAC cím alapú azonosítás már nem tekinthető biztonságosnak.

Egy hálózaton terjedő vírusok és kémprogramok elleni védelem eszközei a fejlett és frissített víruseltávolító programok. A hálózatokon fellépő rendellenes, eltérő, nagy terheléssel járó események szűrésére alkalmas hálózati forgalom elemző és naplózó szoftverek állnak rendelkezésre. Az adatok rendszeres figyelése, a jelenségek értelmezése és felderítése egy belső biztonsági ellenőrzéssel foglalkozó csoport feladata lehet. A kommunikációs hálózatok, illetve a kommunikáció védelme a következő fejezet témája.

A hozzáférések védelme

Amennyiben illetéktelenek férhetnek az eszközökhöz, akkor a rajtuk tárolt adatokat megismerhetik, kinyomtathatják, adathordozóra menthetik vagy elektronikusan továbbíthatják, amivel az adatok tulajdonosának vagy az érintett személyeknek kárt okozhatnak. Ezért az eszközökhöz, hálózatokhoz, és adatokhoz történő hozzáférést szabályozni célszerű. A legelterjedtebb megoldás a jelszavas vagy belépőkártyás védelem. A hozzáféréseket célszerű naplózni és naplóbejegyzéseket rendszeresen elemezni annak felderítésére, hogy történnek-e szükségtelen, kockázatos vagy jogosulatlan belépések. Vannak olyan rendszerek, amelyek a nyomtatásokat, perifériákra másolást (pl. Pen Drive), vagy email csatolásokat is felügyelik és naplózzák.

Katasztrófaterv készítése

Egyre nagyobb teljesítményű és komplexitású számítógépes rendszerek esetén megnövekszik az előre nem látható incidensek lehetősége. Ebbe a természeti katasztrófáktól kezdve az elemi károkig, balesetekig, és súlyos hardver problémákig minden beletartozik. A katasztrófákra lehet tudatosan, előre készülni és terveket kidolgozni arra az esetre, amikor rövid időn belül teljesen új alapokon kell elindítani a számítógépes rendszereket. Katasztrófatervek készítését általában megkövetelik a különböző biztonsági szabványok. Ezeket célszerű néha kipróbálni – akár csak papíron, de esetenként élesben is. A katasztrófaterv arra is jó, hogy abban össze vannak gyűjtve mindazok a fontos paraméterek, konfigurációk, jelszavak, mentéseket tartalmazó adathordozók száma és helye, az egyes visszaállítások időtartama, konfigurációja, amik segítik a tervezést, éles helyzetekben pedig alkalmasak prognózisok készítésére. A katasztrófaterv a szükséges személyek, hatáskörök, kul-

csok, hozzáférések gyűjteménye is, ami segít abban, hogy egy vészhelyzet esetén kiket kell kiértesíteni és milyen sorrendben.

Belső adatvédelmi felelős

A teljes intézményi adatkezelési folyamat folyamatos felügyelete kiszűrheti a gyenge láncszemeket, felfedi az esetleges biztonsági réseket. Az intézményi belső adatvédelmi felelős folyamatosan figyelemmel kíséri az adatutakat, javaslatot tehet a párhuzamosságok megszüntetésére, egyes adatkezelések tiltására, folyamatok átszervezésére. Az adatvédelmi törvény 31/A. §-a szerint egyes intézményekben kötelező belső adatvédelmi felelős kinevezése. A törvény szerint az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál; pénzügyi szervezetnél; távközlési és közüzemi szolgáltatónál kötelező a belső adatvédelmi felelős. Egészségügyi intézményekben is kötelező belső adatvédelmi felelőst kinevezni, de ezt az Eüaktv. 32. §-a írja elő. A belső adatvédelmi felelősök feladatait a törvény is megszabja, de ezen felül az intézmények további teendőkkel is megbízhatják. Javaslatára egyre újabb védelmi technikákat vezethetnek be, amellyel növelhetik az adatkezelés biztonságosságát. Párhuzamosságok, adatszivárgásokat, incidenseket fedezhet fel, amelyek sérthetik az adott intézmény és persze az érintett személyek érdekeit. Működésének azonban megelőző szerepe is kell legyen, azaz az újabb technológiákra a dolgozókat megtanítja, az adatok védelmét szolgáló megelőző intézkedéseket javasolhat, feltárhat fogyatékosságokat az elektronikus rendszerekben. A már lejárt megőrzési idejű adatok ellenőrzött megsemmisítését is végrehajtja.

Ellenőrző kérdések

1. Van-e törvényi kötelezettség a személyes adatok biztonságos tárolására?
2. Mi a célja egy információbiztonsági szabványnak?
3. A vállalatok életében miért lényeges a számítástechnikai rendszerek védelme?
4. Részletezze, hogy milyen létesítményvédelmi intézkedések célszerűek egy értékes adatokat tároló rendszer esetén?
5. Milyen módon lehet egy számítóközpont folyamatos és biztonságos kommunikációs képességét fenntartani?
6. Milyen fizikai környezeti hatások veszélyeztethetik a számítástechnikai eszközök működését?
7. Milyen módon lehet biztonságosan tárolni és továbbítani az adathordozókat?
8. Milyen módszerek vannak a hálózati kliensek azonosítására?
9. Milyen eszközökkel korlátozhatók a hozzáférések adatbázisokhoz, fájlokhoz, nyomtatóhoz?
10. Mit tartalmaz a katasztrófaterv, és mi a célja?
11. Milyen előnyöket nyújthat egy belső adatvédelmi felelős alkalmazása?

12. Az anonimizálás alkalmazásának adatvédelmi kérdései

Tudományos kutatás és üzletszerzés érdekében lehetséges személyes adatokat feldolgozni. Az ilyen célok érdekében történő adatkezeléskor is be kell azonban tartani az adatvédelmi törvény szabályait. Ez korlátozásokat jelent, amit az adatokat feldolgozó szervezeteknek be kell tartani – itt leginkább az adatokhoz történő hozzáférés okozza a problémát, ugyanis olyan harmadik személyek szereznének tudomást személyes adatokról, akik erre nem lennének jogosultak pl. tanácsadó cégek, piackutató intézetek, kutató kollektívák. Nem véletlen, hogy az adatkezelők szeretnének olyan módszereket alkalmazni, amellyel kivonhatják magukat az adatvédelmi törvények hatálya alól. Az erre kínálkozó egyik megoldás az, hogy ha az adatok *személyes* jellegét megszüntetik. Vagyis olyan átalakítást hajtanak végre az adatokon, amely után az adatok nem kapcsolhatók össze egy élő személlyel. Az Avtv. nem adja meg az anonimizálás definícióját, ugyanakkor szerepel a szövegében:

> 32. § (1) Tudományos kutatás céljára felvett vagy tárolt személyes adat csak tudományos kutatás céljára használható fel.
>
> (2) A személyes adatot – mihelyt a kutatási cél megengedi – *anonimizálni* kell. Addig is külön kell tárolni azokat az adatokat, amelyek meghatározott vagy meghatározható természetes személy azonosítására alkalmasak. Ezek az adatok egyéb adatokkal csak akkor kapcsolhatók össze, ha az kutatás céljára szükséges.
>
> (3) A tudományos kutatást végző szerv vagy személy személyes adatot csak akkor hozhat nyilvánosságra, ha
>
> a) az érintett abba beleegyezett, vagy
> b) az a történelmi eseményekről folytatott kutatások eredményeinek bemutatásához szükséges.

Anonimizálás után – amennyiben azt tökéletesen végzik el – az adatok a továbbiakban már nem fognak az adatvédelmi törvény hatálya alá tartozni. Így az érintettek jogait sem kell a továbbiakban biztosítani. Az anonimizálás ezért komoly szakmai és jogi felelősséget jelent. Ha nem kellő körültekintéssel hajtják végre, azaz ha az érintettek személye meghatározható, akkor annak beláthatatlan következményei lehetnek főként nagyobb állományok esetén. Illetéktelen kezekbe kerülve, egyszerre nagyszámú érintett magánéletét sodorják veszélybe. Paul Ohm a Coloradoi Egyetem kutatója *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* című cikkében[61] három esetet ismertetett, amelynek során az Egyesült Államokban elvileg anonimizált adatbázisokat törtek fel, az interneten található egyéb adatokkal történő összekapcsolás módszerével. Az AOL Research (kapcsolati kóddal ellátott) adatait, amely az adott felhasználó összes webkeresőben feltett kérdéseit tartalmazta; a második esetben a massachusettsi GIC (Group Insurance Commission) egészségbiztosító kapcsolati kódolt adatbázisát törte fel egy egyetemista a szavazásra jogosultak nyilvános adatbázisát felhasználva és sikeresen azonosította benne a kormányzó egészségügyi adatait; a harmadik eset egy online video kölcsönző, a Netflix kapcsolati kódolt adatbázisának a feltörése volt.

[61] http://lawweb.colorado.edu/profiles/profile.jsp?id=180

A humángenetikai vizsgálatokról és kutatásokról szóló 2008. évi XXI. törvény 3. § (1) bekezdés f) pontjában szereplő definíció is pontatlan ebből a szempontból:

> f) anonimizált genetikai minta vagy adat: olyan genetikai minta vagy adat, amellyel kapcsolatban az érintettre vonatkozó összes személyazonosító adatot személyazonosításra alkalmatlanná tettek;

Nyilvánvaló, hogy a személyazonosító adatok (név, anyja neve, születési hely és idő, lakcím) egyszerű eltávolítása nem jelenti azt, hogy az érintett, akire az adatok vonatkoznak nem azonosítható. Elegendő pl. az életkor, falu/város, nem, betegségkód a pontos személyazonosításhoz. Genetikai mintánál elegendő egy ritka genetikai tulajdonság, de maga a genetikai ujjlenyomat is az azonosításhoz. A személyes egészségi adatokon végzett kutatások meglehetősen gyakoriak, mivel jelentős mennyiségű adat halmozódott fel az évek során. Ugyanakkor mivel ezek különleges személyes adatok – az adatvédelemnek is kitüntetett szerepet kell kapnia. Ráadásul, a kutatásoknak egyes esetekben fontos következményei lehetnek a páciensek további sorsára nézve, ezért az adatokat nem fosztják meg véglegesen a személyazonosítás lehetőségétől, hanem kódolják (pszeudonimizálják). Ez azt jelenti, hogy az adatsorokhoz kódszámot rendelnek, és megőrzik a kódszámokhoz tartozó személyek adatait is. A kódkulcshoz a kutatók nem férhetnének hozzá, csak fontos egészségügyi érdekből, amikor feltétlenül fel kell venniük az érintettel a kapcsolatot.

Az Egyesült Államokban 1997-ben fogadták el a HIPAA (Health Insurance Portability and Accountability Act, Egészségbiztosítások hordozhatóságáról és elszámolhatóságáról szóló szövetségi) törvényt. Ennek az volt a célja, hogy az állampolgárok bármely szövetségi államban azonos módon vehessenek igénybe egészségügyi ellátásokat. Bár szövetségi adatvédelmi törvény nincs az USA-ban, azonban a HIPAA törvény részletesen foglalkozik az egészségügyi adatok bizalmas kezelésével. A törvény szerint csak akkor tekinthető egy adathalmaz anonimnak, ha a jövőre nézve sem merül fel semmilyen kétség, hogy valaha is az adatokat konkrét elő személyekhez kapcsolhatják. Ennek megakadályozására szolgáló egyik eszköz a személyek és a kódok kapcsolatát tartalmazó lista megsemmisítése. A kódolást gyakran azért alkalmazzák, hogy ha valamilyen fontos egészségügyi célból el kellene érni a kutatás egyes résztvevőit, akkor ezt meg lehessen tenni. Amikor azonban a kutatás véget ér, a listára már nincs szükség, meg lehet azt semmisíteni.

A HIPAA törvény melléklete felsorolt számos olyan adatot, amelynek a jelenléte megkönnyíti a személyazonosítást, ezért ezeket anonimizáláskor feltétlenül el kell távolítani az adatokból. Ezt a felsorolást tartalmazza Carole Lucock ügyvédnő, University of Ottawa írása: Anonymization of Electronic Health Information Data. Eszerint nincs helye az adatok között semmilyen névnek (orvos nevének sem), dátumnak (csak évszámok megengedettek), az életkort években kell megadni, 90 év felett azt sem. Az adatok között semmilyen cím nem szerepelhet (kizárólag irányítószám, amely nem mutat 20 ezer főnél kisebb földrajzi egységre), nem szerepelhet semmilyen telefonszám, faxszám (intézményé sem), rendszám, e-mail cím, gép vagy berendezés gyári száma, arcot is tartalmazó fénykép. Az az anonimizálás, amelynek során egyedül a TAJ számot távolítják el, az egészségügyi rekordokból láthatóan a HIPAA útmutató több lényeges pontját sérti meg, ezért egy ilyen adatbázis nem tekinthető anonimnak.

Vajon az így kódolt, idegen szóval pszeudonimizált adatok személyes adatok-e? Az ilyen adatok kétféle módon lehetnének személyhez kapcsolhatók. Az egyik mód, ha a kódok és a személyek kapcsolatát leíró listát meg lehetne szerezni, a másik mód, ha az adatok között előforduló több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális

azonosságra jellemző tényező segítségével azonosítani lehet az érintetteket. Például, az irányítószám, eredet, életkor, testsúly előfordulása az adatok között eredményezhet azonosíthatóságot egy kisebb magyar település esetén. Ráadásul az azonosításhoz nem kell szükségképpen orvosnak lenni, elég, ha valaki általános iskolai tanár, önkormányzati ügyintéző stb. Ezért az EuroSOCAP szabvány[62] szerint a kódolás csupán kiegészítő védelmet nyújt a személyes adatok bizalmas feldolgozásakor, de az adatok személyes jellegét nem szünteti meg. Ezért a szabvány 3.3.5. pontjában ez áll:

> Az anonimizálás nem jelent alternatívát a kifejezett beleegyezés megszerzésével szemben, inkább csak egy kiegészítő védelemnek tekinthető ahhoz, hogy bizalmas maradjon az az információ, amelyet felhasználni és továbbítani csak beleegyezés birtokában lehet. Az anonimizálás a 95/46/EK irányelv szerint kiveszi az adatokat az irányelv alapelveinek hatálya alól. Az adminisztrátoroknak és a kutatóknak különösen fontos érdekük fűződik ahhoz, hogy arra hivatkozzanak, hogy az adatokat, amelyeket feldolgoznak anonimizálták az irányelv 26. pontja szerint. Ám ezeknek az elveknek alapján, a személyes adatok csak akkor tekinthetők anonimizáltnak, ha a továbbiakban senki (sem az adatkezelő sem bárki más) nem azonosíthatja az érintettet magukból az adatokból vagy az adatokból kombinálva azokat bármilyen más eszköz felhasználásával, amely nagy valószínűséggel lehetővé teszi, hogy az érintett személyazonosságát felfedjék. Így például, ha a kutató olyan formában tárolja az adatokat, hogy ő maga nem tudja azonosítani az érintettet, de más valakinek a birtokában van egy kód, amely lehetővé teszi ezt, akkor a kutató által végzett adatfeldolgozás már nem anonimizált adatokon történik. Az sem ismeretlen a kutatók számára, hogy akkor is hivatkozzanak arra, hogy anonimizált adatokon végeznek feldolgozást, ha mások vagy akár saját maguk is különböző egyszerű eszközökkel azonosítani tudják az érintettet. Például a kutatók általában gyakran mondják egy adatra, amelyhez nem csatolták az érintett nevét, hogy anonim. A gyakorlatban az ‘anonimizált’ jelzővel illetni az adatokat egy értékítélet, és a kutatóknak egyáltalán nem szabadna ezt használni ebben ez értelemben, hanem egyszerűen le kellene írniuk, hogy milyen formában tárolják és dolgozzák fel az adatokat, az etikai bizottságokra és az érintettekre hagyva annak eldöntését, hogy mekkora jelentősége van ennek.
>
> Ha valaki tisztességesen szeretné anonimizálni az információt, akkor a legjobb, ha biztosítják, hogy törvényesen és etikusan járjanak el, és tájékoztatják a pácienseket és/vagy törvényes képviselőiket erről a szándékukról és hogy ennek milyen hatása lehet, különösen arra nézve, hogy a páciensek hogyan férhetnek hozzá az adataikhoz és hogy tudhatják meg hogy az adataikat mire használják fel (és így tiltakozhassanak az ilyen felhasználások ellen). Ez azért van, mert a 95/46/EK irányelv megköveteli, hogy az érintetteket tájékoztassák minden egyes feldolgozás céljáról és maga az anonimizálás is a személyes adatok egy feldolgozása. Sőt, az ilyen előzetes tájékoztatás nem ad felmentést az alól sem, hogy az érintettet arról is tájékoztassák, hogy az anonimizálás után mi az adatok feldolgozásának szándékolt célja. Az anonimizálást olyan esetekben kell használni, amikor adatokat nem szükséges személyes formában tárolni és nem ismert, hogy az adatokat milyen célokra fogják esetleg felhasználni.

[62] A szabvány letölthető a következő webcímről: http://www.orpha.net/testor/doc/july05/EuroSOCAP.pdf

Az adatok feltörésére kínálkozik még egy módszer: az eredeti adatokhoz történő visszacsatolás. Tehát, ha kideríthető, hogy egy táblázat mely kórháztól vagy klinikától származik, és szerepel néhány dátum, számadat, laboratóriumi eredmény az adatok között, akkor a kódolt táblázatot összehasonlítva a kórházban tárolt adatokkal ismét helyreállítható az érintettekkel a kapcsolat. Erre különösen akkor van esély, ha a kódolt táblázatot már nem tekintik személyes adatnak, és így az bárki, de leginkább az érintett szakma képviselői számára szabadon hozzáférhetővé, terjeszthetővé válik.

Az Európai Bizottság 29. cikk alapján létrehozott munkacsoportjának a személyes adatokról készített WP 136 számú munkadokumentuma szerint, amennyiben valóban nem juthat el a kódok és személyek kapcsolatát tartalmazó lista az adatkezelőhöz (pl. mert az adatkezelő egy másik távoli országban van), és az adatok a fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényezők alapján sem azonosíthatók, akkor megfelelő biztonsági intézkedések mellett tekinthetők személyazonosításra alkalmatlan (anonim) adatoknak.

A név, cím, születési adatok eltávolítása az adatokból nem elegendő. Ahhoz hogy valóban anonim adatokat kapjunk leginkább az szükséges, hogy nagyszámú adattal dolgozzunk. Ha az adatok száma nagy, és a számadatok alapján egyetlen személy nem (hanem mondjuk 38 vagy 53) lenne azonosítható, akkor már egyre közelebb kerülhetünk ahhoz, hogy azonosíthatatlan adatokat kapjunk. Matematikusok[63] vezették be az ún. *k*-anonimitás fogalmát amely szerint, ha bármely kiválasztott számadathoz legalább *k* személy tartozhat, és a *k* nagyobb mondjuk 100-nál, akkor az a táblázat már valószínűleg nem tartalmaz személyes adatokat. Egy konkrét táblázat esetén a *k* értékét ki lehet számítani, az érték nagysága jól jellemzi a táblázat feltörhetőségét a későbbiekben. Az USA-ban azt feltételezik, hogy a kutatási adatok mellé a kutatók valószínűleg meg tudják szerezni az eredeti betegadatokat is és a két számsor összevetésével azonosítani tudják a személyeket is.

Van-e olyan kutatási projekt, amely nem valósítható meg személyes adatok kezelése nélkül, bár a kutatóknak a végén az azonosíthatóságra nincs szükségük. Erre a válasz az, hogy igen. Előfordulhat, hogy több különböző egészségügyi intézményből kellene adatokat gyűjteni úgy, hogy az egy páciensheztartozó adatokat össze lehessen kapcsolni (vagy az egy páciensheztartozó ismétlődő adatokat ki lehessen szűrni). Azonban az adatgyűjtés megtörténte után már nincs szükség az azonosíthatóságra. A fenti gondolatmentet követve erre csak írásbeli beleegyezés birtokában lenne lehetőség, mivel személyes adatokat használnának fel kutatási célokra. Hogy ezt a problémát meg lehessen oldani az egyéni önrendelkezés különösebb megsértése nélkül, például az Egyesült Királyságban 2003-ban módosították az Egészségügyi törvényt olyan módon, hogy a kimaradás jogával élni nem kívánó páciensek adatait az egészségügy miniszter rendeletére, komoly etikai és adatvédelmi garanciák mellett, egy független intézmény összekapcsolhatja, majd miután megfosztotta az azonosíthatóságtól, az adatokat a kutatóknak átadhatja.

Anonimizáláskor arra is figyelemmel kell lenni, hogy ilyen esetben az érintettek adatvédelemhez fűződő jogát teljes mértékben elvonják, ugyanakkor a műveletet úgy hajtják végre, hogy az adatkezelő (kutatók) a maguk számára a legelőnyösebb és korlátozás nélküli felhasználást biztosíthassák. Ezért az anonimizálás nem utolsó sorban etikai kérdés is, amelyet indokolt független hatóságnak is ellenőriznie. Franciaországban és az Egyesült Királyságban is az orvosi kutatásokat nem csak etikai szempontból véleményezik, hanem adatvédelmi hatósági jóváhagyás is minden esetben szükséges az engedélyezéshez, ha nem

[63] Lásd Johannes Gehrke (Cornell University) publikációi és honlapja: http://www.cs.cornell.edu/johannes/

áll rendelkezésre írásos hozzájárulás az érintettek részéről. Az Egyesült Királyság adatvédelmi biztosa már 1998-ban úgy foglalt állást, hogy az anonimizálás adatkezelésnek számít, hiszen az adatokon végzett művelet, és kizárólag megfelelő törvényi alap, vagy hozzájárulás mellett végezhető. A mai napig ezt az állásfoglalást figyelembe veszik a jogalkotási folyamatban. Szövetminták esetén ugyancsak fontos kérdés, hogy amikor a mintáról a címkét lekaparja valaki, onnantól kezdve a mintával bármit tehet-e, megfoszthatja-e az érintetteket minden adatvédelemhez fűződő joguktól?

Létezik-e egyáltalán azonosíthatatlan biológiai minta?

Ez a kérdés azért fontos, mert általában a biológiai mintákat addig tekintik személyes adatnak (lásd. Avtv 2. § 1. és 9. pont), amíg a kapcsolat a minta és egy létező személy között helyreállítható. Amikor a mintát azonosító számsort letörlik, akkor vajon a minta ezáltal azonosíthatatlanná vált-e? Elméletileg természetesen nem, hiszen a személyazonosításra rendelkezésre állnak már genetikai módszerek, amelyekkel az azonosítás kétséget kizáróan elvégezhető. Tekintettel azonban arra, hogy ehhez szükséges lenne az összes szóba jöhető személy ellenőrzött genetikai vizsgálatára (genetikai ujjlenyomat vétellel), hogy közülük ki lehessen választani az adott személyt, ez aránytalanul nagy erőfeszítés lenne, mivel drága, elvégzésének kicsi a kockázata, ezért a gyakorlatban esetleg lehetne a mintát azonosíthatatlannak tekinteni (amely ez után már nem személyes adat).

Az ismeretlen minta azonosítására azonban nemcsak ez a lehetőség áll rendelkezésre, hanem olyan genetikailag kódolt tulajdonságok is, amelyek az ismeretlen személy megfigyelhető külső jellegzetességeit alkotják, pl. a vércsoport, szem szín. Az ilyen genetikailag kódolt tulajdonságok száma folyamatosan növekszik, ezért nem lehet garantálni, hogy ami ma esetleg nem azonosítható minta az a jövőben is az marad. Különösen igaz ez akkor, ha az ismeretlen minta valamilyen határozott genetikai rendellenességet mutat, amelynek esetleg jól felismerhető külső megnyilvánulásai is vannak. Ebben az esetben már az azonosítás sokkal egyszerűbb. Az azonosítást további információk is segíthetik: az egészségi állapotra vonatkozó egyéb adatok. Az orvosi genetikai kutatások nagyon fontos eleme, a génekben kódolt tulajdonságok és az egészségi állapot közötti kapcsolat kimutatása, vizsgálata. Természetesen, kutatási célból csak olyan biológiai minta felhasználása érdekes, amely együtt jár az egészségi állapotra vonatkozó adatok átadásával is, egyébként a minta valószínűleg érdektelen a kutatások szempontjából.

Az adatvédelmi törvény szerint annak ellenőrzéséhez, hogy egy adathalmaz létező személyhez kapcsolható-e fel kell tárni, hogy milyen egyéb adatok állnak az adatkezelő rendelkezésére, illetve, hogy milyen további adatok megszerzésére van lehetősége, vagy milyen adatokra tehet szert a jövőben. A szöveteket tároló biobankok sok esetben gyógyintézetek, klinikák mellett, esetleg azokkal egy szervezeti egységben működnek, amelyek közös informatikai rendszert működtetnek. Nem alaptalan az a feltételezés, hogy ezeket az adatokat össze is lehet kapcsolni. A fentiekből az a következtetés adódik mindent figyelembe véve, hogy *azonosíthatatlan biológiai minta nem létezik*. Addig, amíg az érintett él, vagy az egészségügyi adatai léteznek, addig biztosan nem. A halál után 30-50 évvel esetleg már valóban azonosíthatatlanná válik egy minta. Az elkövetkező néhány évben a könnyű és gyors azonosíthatóság majdnem biztosan bekövetkezik. Az is jól megfigyelhető a humángenetikai törvényjavaslatban, hogy kutatási érdek az, hogy teljesen szabadon felhasználható mintákat kaphassanak a kutatók, amelyek az érintett engedélyével, vagy még inkább a törvény felhatalmazása alapján már korlátozás nélkül felhasználhatók. Ennek legjobb módja a név nélküli minták használata (amelyek a törvényjavaslat vélelmezése szerint

nem azonosíthatók, tehát nem tekinthetők személyes adatnak). A törvényjavaslat szerint a jelenleg különböző helyeken őrzött, tárolt (nyilvánvalóan megsértve ezzel az 1997. évi CLIV. törvény előírásait) biológiai mintákat, a rajtuk lévő azonosítók letörlésével szabadon felhasználható biológiai mintákká lehetne minősíteni. Ez az elgondolás nincs összhangban azzal, az Ovideoi Egyezményben kinyilvánított alapelvvel, hogy az egyéni érdek megelőzi a tudományos és társadalmi érdeket, ezen kívül minimum kimeríti a tisztességtelen adatkezelés fogalmát. Ezeket a mintákat már régen meg kellett volna semmisíteni, és a véleményem szerint ezt kell tenni most is, haladéktalanul meg kellene semmisíteni őket. A törvényjavaslat nem gondoskodik arról, hogy a biobankban tárolt mintákat ne lehessen azonosíthatatlanná tenni, amely a véleményem szerint nagyon súlyos etikai és emberi jogi kérdés. Ezt a cselekményt nem szankcionálja a törvény, pedig megelőzhető lenne, ha minta adományozásakor, minden adományozó elvégeztetne egy személyazonosító genetikai tesztet is, amelynek az eredményét egy-egy példányban megkapná a biobank és az érintett. Ennek birtokában később bármikor lehetne azonosítani a mintákat, még akkor is, ha esetleg elveszne róluk a címke. Ennek a tesztnek a puszta létezése (a benne foglaltak ismerete nélkül is), azonnal eloszlatná azt a kételyt, hogy a név nélkül tárolt biológiai minta személyes adat-e vagy sem.

Nyílt genetikai adatbázisok

A nemzetközi genetikai kutatások során általános gyakorlat, hogy szabadon hozzáférhető adatbázisokat készítenek. Ezeket az Interneten keresztül érik el a kutatók Egyiptomtól kezdve Brazíliáig. A genetikai adatbázisokban a genom egyes szakaszai, DNS részletek aminosav szekvenciái találhatók. Általános alapelv, hogy adatokat ezekbe az adatbázisokba csak beleegyező nyilatkozat birtokában lehet felvinni. Ennek a törvényi szabályozását nem találtam meg a törvényjavaslatban. Pontosabban szólva, ennek a kérdésnek az adatvédelmi törvény vagy az Egészségügyi adatkezelési törvény alapján kellene megoldódni. Ha betű szerint alkalmazom ezeket a törvényeket, akkor nem azonosítható adatokat az adatbázisba fel lehet vinni az érintett beleegyezése nélkül is. Ez a véleményem szerint ismét sérti a tisztességes adatkezelés elvét, továbbá, számos jövőbeli kockázatot is magában rejt.

A genetikával foglalkozók ismerik a világban található genetikai adatbázisokat, és megfelelően gyors keresőprogramok állnak rendelkezésükre egy-egy adatbázisban tárolt adat előkeresésére. Ezért, ha egy adott páciens genetikai vizsgálatra jelentkezik, miközben korábban a biológiai mintáján orvosi kutatásokat végeztek és annak eredményét nemzetközi, nyílt adatbázisban helyezték el, akkor a frissen keletkezett adatok és az adatbázis tartalmának az összekapcsolásával olyan ismeretek kerülhetnek a felszínre, amelyek esetleg a páciens szándéka ellenére vannak. A véleményem szerint az Interneten történő közzététel nyilvánosságra hozásnak számít, amely csak egyedi speciális engedély birtokában lehetséges. Ezt úgy kellene bővíteni, hogy genetikai vizsgálatok eredményét akkor, ha az azokban fellelhető információmennyiség elvben személyazonosításra alkalmas (azt a gyakorlati szempontot nem vizsgálva, hogy ez mennyire nehéz), csak egyedi beleegyezés birtokában lehetne nyilvános adatbázisban közzétenni.

Ellenőrző kérdések

1. Mi az anonimizálás célja?
2. Végrehajtható-e tökéletes anonimizálás?

3. Említsen példákat arra, amikor anonim adatbázisokat sikerült feltörni!
4. Mit jelent a pszeudonimizálás, és a kódolás?
5. Miért lehet szükség anonimizálás helyett pszeudonimizálásra?
6. Mit tartalmaz az ún. HIPAA útmutató?
7. Mi az álláspontja az EuroSOCAP szabványnak az anonimizálásról?
8. Mi a k-anonimitás definíciója?
9. Miért etikai probléma az anonimizálás?
10. Adatfeldolgozásnak számít-e az anonimizálás?
11. Létezik-e azonosíthatatlan biológiai minta?
12. Milyen veszélyekkel járnak a nyilvános genetikai adatbázisok?

13. A magyar adatvédelmi biztosok munkássága

Az Európai Parlament és a Tanács 95/46/EK (1995. október 24.) adatvédelmi irányelvének 28. cikke kötelezővé tette minden tagállam számára egy adatvédelmi *felügyelő hatóság* létrehozását. Ez a rendelkezés alapvetően meghatározta ennek a felügyelő hatóságnak a tevékenységi körét, előírja a hatóság független működését, hogy a hatóságnak hozzáférési joga van bármely adatállományhoz (legyen az akár titkos), legyen beavatkozási és megrovási joga, bírósági eljárásban részvételi joga. Az irányelv tartalmazza, azt, hogy a felügyelő hatósághoz bármely személy fordulhasson, illetve hogy a felügyelő hatóság intézkedései ellen legyen jogorvoslati lehetőség. Ez a hatóság Magyarországon az Adatvédelmi Biztos Hivatala (1051 Budapest V. kerület, Nádor u. 22.)

> 28. cikk
> A felügyelő hatóság
>
> (1) Minden tagállamnak rendelkeznie kell arról, hogy az ezen irányelv értelmében a tagállam által elfogadott nemzeti rendelkezéseknek a területén történő alkalmazását valamely hatóság vagy hatóságok felügyeljék.
>
> E hatóságok a rájuk ruházott feladatok gyakorlása során teljes függetlenségben járnak el.
>
> (2) Minden tagállamnak rendelkeznie kell arról, hogy a személyes adatok feldolgozása vonatkozásában az egyének jogainak és szabadságainak védelmére vonatkozó közigazgatási intézkedések vagy rendeletek kidolgozásakor a felügyelő hatóságokkal konzultáljanak.
>
> (3) A hatóságok különösen a következő jogosultságokkal rendelkeznek:
>
> - vizsgálati jogkör, mint például az adatfeldolgozási műveletek tárgyát képező adatokhoz való hozzáférés joga, továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének joga,
>
> - tényleges beavatkozási jogosultságok, mint például a 20. cikknek megfelelően végzett adatfeldolgozási műveletek megkezdése előtti véleményezés joga, e vélemények megfelelő közzétételének biztosítása, az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése, az adatfeldolgozás átmeneti vagy végleges tilalmának megállapítása, az adatkezelő figyelmeztetése vagy megrovása, illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése,
>
> - bírósági eljárásban való részvétel joga az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén, továbbá e jogsértések igazságszolgáltatási hatóságok elé terjesztésének joga.
>
> A felügyelő hatóság kifogásolható határozatai bíróság előtt megtámadhatók.
>
> (4) A felügyelő hatóságok foglalkoznak a személyes adatok feldolgozása vonatkozásában az egyének jogainak vagy szabadságainak védelmével kapcsolatos, bármely személy vagy az őt képviselő szervezet által benyújtott kérelmekkel. A kérelem elbírálásáról az érintett személyt értesíteni kell.

> A felügyelő hatóságoknak foglalkozniuk kell különösen az adatfeldolgozás törvényességének ellenőrzésére irányuló, bármely személy által benyújtott kérelemmel, amennyiben az ezen irányelv 13. cikkének értelmében elfogadott nemzeti rendelkezések alkalmazhatóak. Az érintett személyt mindenképpen értesíteni kell, ha az ellenőrzés megtörtént.
>
> (5) A felügyelő hatóságok tevékenységükről rendszeresen jelentést készítenek. A jelentést nyilvánosságra kell hozni.

A magyar adatvédelmi biztost, a fent említett hivatal vezetőjét a Parlament választja meg 6 éves megbízatással. A javaslattételt, a választás menetét, a biztos jogállását, mentelmi jogát, megbízatásának megszűntét és működését az állampolgári jogok biztosáról szóló 1993. évi LIX. törvény szabályozza általában. Az adatvédelmi biztos megválasztását a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény IV. fejezete írja le:

> Avtv. 23. § (1) A személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében az Országgyűlés adatvédelmi biztost választ azok közül az egyetemi végzettségű, büntetlen előéletű, kiemelkedő tudású elméleti vagy legalább 10 évi szakmai gyakorlattal rendelkező magyar állampolgárok közül, akik az adatvédelmet érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében jelentős tapasztalatokkal rendelkeznek.
> (2) Az adatvédelmi biztosra – e törvényben foglalt eltérésekkel – az állampolgári jogok országgyűlési biztosáról szóló törvény rendelkezéseit kell alkalmazni.
>
> 24. § Az adatvédelmi biztos
> a) bejelentés alapján vagy – ha az adott ügyben bírósági eljárás nincs folyamatban – hivatalból ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok megtartását;
> b) kivizsgálja a hozzá érkezett bejelentéseket;
> c) gondoskodik az adatvédelmi nyilvántartás vezetéséről;
> d) elősegíti a személyes adatok kezelésére és a közérdekű adatok nyilvánosságára vonatkozó törvényi rendelkezések egységes alkalmazását;
> e) feladatkörében általános jelleggel, valamint meghatározott adatkezelő részére ajánlást bocsáthat ki;
> f) véleményezési jogot gyakorol az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv tevékenységével kapcsolatosan külön törvényben meghatározottak szerint közzéteendő adatokra vonatkozó különös, illetőleg egyedi közzétételi listák tekintetében;
> g) külön törvényben meghatározott szervekkel vagy személyekkel együttműködve képviseli a Magyar Köztársaságot az Európai Unió közös adatvédelmi felügyelő testületeiben;
> h) gyakorolja és ellátja az e törvényben meghatározott hatásköröket és feladatokat.
>
> 24/A. §
> (1) Az adatvédelmi biztos eljárására és intézkedéseire az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény (a továbbiakban: Obtv.) rendelkezéseit az e törvényben meghatározott eltérésekkel kell alkalmazni.

> (2) Az adatvédelmi biztos eljárására az Obtv. 16. § (1) és (2) bekezdését, 17. § (3) és (4) bekezdését, 18. § (1), (6) és (8) bekezdését nem kell alkalmazni.

Magyarországon több országgyűlési biztos is működik: a jövő nemzedékek országgyűlési biztosa, a nemzeti és etnikai kisebbségi jogok biztosa, állampolgári jogok biztosa és az adatvédelmi biztos. Mindannyijuk tevékenységét szabályozza a nevében kissé félrevezető Obtv., a állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény. Ebben szerepel az, hogy általában akkor indít eljárást a biztos, ha a panasztevő már élt a számára biztosított jogorvoslati lehetőségekkel, azokat kimerítette és más lehetőség nem lévén, a biztosi hivatalhoz fordult. Ez az alapfeltétel az adatvédelmi biztos esetére nem vonatkozik. Ez a hivatal akkor is eljár, ha az érintett nem élt még jogorvoslati lehetőséggel. Az Obtv. Ide vonatkozó paragrafusa:

> Obtv. 16. § (1) Az országgyűlési biztoshoz bárki fordulhat, ha megítélése szerint valamely hatóság [29. § (1) bek.], illetve közszolgáltatást végző szerv (a továbbiakban együtt: hatóság) tevékenysége során a beadványt benyújtó személy alapvető jogaival összefüggésben visszásságot okozott, feltéve, hogy a rendelkezésre álló közigazgatási jogorvoslati lehetőségeket – ide nem értve a közigazgatási határozat bírósági felülvizsgálatát – már kimerítette, illetve jogorvoslati lehetőség nincs számára biztosítva.
> (2) Az országgyűlési biztos az alapvető jogokkal kapcsolatos visszásság megszüntetése érdekében az (1) bekezdésben megjelölt feltételek fennállása esetén hivatalból is eljárhat.
> (3) Az országgyűlési biztoshoz benyújtott minden beadvány illetékmentes.
> (4) Ha a beadványt benyújtó személy kéri, kilétét az országgyűlési biztos nem fedheti fel. Az országgyűlési biztoshoz fordulása miatt senkit sem érhet hátrány.

Az Obtv. Intézkedik arról, hogy a biztosokhoz a panaszt az utolsó jogorvoslati lehetőség kimerülése után 1 éven belül kell előterjeszteni, a biztos számára mindenki köteles felvilágosítást adni, a biztos hozzáférhessen titkos adatokhoz, titoktartási kötelezettsége legyen stb.

13.1. A magyar adatvédelmi biztosok

Dr. Majtényi László: (1995. június 30. – 2001. június 30-ig)

1950. november 30-án született Budapesten. Jogász, az Eötvös Károly Közpolitikai Intézet elnöke, a Pécsi Tudományegyetem docense. Három gyermeke és négy unokája van, felesége legfelsőbb bírósági bíró.

Felsőfokú végzettség: jogász, ELTE ÁJK, 1975.

Tudományos fokozatok

– egyetemi doktori fokozat (dr. univ.): 1975. ELTE ÁJTK

Doktori disszertációjának témája: A normaelsajátítás típusai

– az állam és jogtudomány kandidátusa (PhD): 1992,

Témája: Ombudsman: Állampolgári Jogok Biztosa

Szakmai életútja:

– Jogi előadó, Jogtanácsos, MAHART 1975-1980
– Ügyvédi, jogtanácsosi szakvizsga, 1978
– A Műegyetem oktatója, egyetemi adjunktus 1980, egyetemi docens (-1992)
– A Műszaki Egyetem Jogtudományi Osztályának vezetője 1992-1995
– Az Alkotmánybíróság tanácsadója, főtanácsadója: 1990-1995
– A Magyar Köztársaság adatvédelmi biztosa 1995-2001
– A Világosság társadalomtudományi folyóirat szerkesztője 1974-, majd később a szerkesztőbizottság tagja -1995
– A Fundamentum c. folyóirat alapító szerkesztője
– A Budapesti Könyvszemle szerkesztője, 2002-
– A Széchenyi István Egyetem docense, 1995-2002
– Eötvös Károly Közpolitikai Intézet, elnök, 2003-2008
– ORTT elnöke, 2008-2009
– A PTE ÁJK egyetemi docens, 2003-
– Több magyarországi egyetem, felsőoktatási intézmény rendszeres meghívott előadója: ELTE ÁJK, Jogi Továbbképző Intézet, Pázmány Péter Katolikus Egyetem, Mathias Corvinus Collegium, Láthatatlan Kollégium.
– Az egyetemi munkája során oktatott tantárgyak: Alkotmányjog, etika, adatvédelem, információs jogok, ombudsmanintézmények, közlekedési jog, tengeri fuvarjog, szállítmányozás, nemzetközi tengeri és belvízi közjog, hajózási jog, biztosítási jog
– Doktorandusz képzés
– Pázmány Péter Katolikus egyetem 2001-2002
– PTE ÁJK Doktori Iskolája (2003)
– Phd. Bíráló bizottság, PTE ÁJK

Kutatási témái:
– Ombudsman intézmények összehasonlító vizsgálata.
– Az információs társadalom elmélete és jogi környezete.
– Adatvédelem és információszabadság Magyarországon és az Európai Unióban.
– Alkotmányjog
– Alapjogi bíráskodás

Dr. Majtényi László adatvédelmi biztos egy még kiforratlan úton indult el 1995-ben. Akkor még több szektoriális törvény nem állt rendelkezésre pl. az Eüaktv., és a meglévők sem voltak összhangban az Avtv. rendelkezéseivel. 1995-ben az első nagyobb ügye a lottó ötös ügy, amelynek során a rekordösszegű nyeremény tulajdonosaival a tévé riportot készített, és természetesen gyorsan fény derült a nyertesek kilétére (83/H/1995). Az 1995-ös MIÉP tüntetésen videofelvételeket készített a rendőrség – ezzel kapcsolatban adott ki egy ajánlást, amelyben az állt, hogy amennyiben a rendezvényeken jogsértő cselekmény nem történik – úgy a készült felvételeket a legrövidebb időn belül meg kell semmisíteni (118/A/1995). Általános ajánlást is tett a Kaposváron tervezett közterületi kamerás megfigyelő rendszerrel kapcsolatban. Fellépett a Xénia Láz Egyesület adatkezelése ellen, mivel a belépési nyilatkozathoz egy kérdőív is tartozott, amelyen családtagokra, egészségi állapotra, politikai érdeklődésre utaló kérdések voltak és a kitöltött belépési nyilatkozat miatt személyhez kapcsolhatók (450/A/1996). A Dunabank Rt. és az ING Bank Rt. közötti adatátadás körülményeit is vizsgálta, és megállapította, hogy a két bank közötti megállapodás nem teremtett jogalapot az ügyfelek személyes banki adatainak automatikus átadására (439/A/1996).

Állásfoglalást adott ki arról, hogy az újságok a sértetteket egy cikkben nem nevezhetik meg, és az elkövetőket is csak bírósági szakaszban (56/A/1999). A televízió társaságok számára készített igen fontos ajánlást, amely a balesetek, tűzesetek, bűncselekmények helyszínein készült riportok adatvédelmi kérdéseit tisztázta (100/H/1999). Alapvetően a riportalanyok önkéntes beleegyezése szolgáltatja az adatkezelésre a jogalapot. Kiskorú, nem cselekvőképes személy esetén pedig a törvényes képviselő hozzájárulása szükséges. Kifogásolta a bűnüldöző szervek gyakorlatát, amikor az adatkezelőknél személyes adatokat foglalnak le ahelyett, hogy írásban az adatok megküldését kérnék. Ez utóbbinál ugyanis a nyomozó hatóságnak indokolnia kell és csak a minimálisan szükséges adatot kezelheti – szemben a lefoglalással, amikor az adathordozót egészben megszerzik (252/K/2001) – ez a gyakorlat még ma is előfordul. A 2001-es népszámlálás ügyében is hosszabb állásfoglalást tett, amelyben állást foglalt abban, hogy a gyűjtött adatokat nem azonosíthatják a személyi azonosítóval, nem kapcsolhatják össze más adatbázisokkal, és nem továbbíthatják más feldolgozónak (139/A/2001).

A TASZ társadalmi szervezet beadvánnyal fordult az adatvédelmi biztoshoz, amiért a rendőrség razziákat tartott egy drogambulancián és betekintett a kezelt páciensek egészségügyi adataiba (172/A/1996). A gyógyszertárakból az OEP felé továbbított adatok tekintetében egy ajánlást tett, amely szerint a gyógyszertárak csak személyazonosításra alkalmatlan módon továbbíthatnák a gyógyszer kiváltásáról az adatokat – ezt a mai napig nem vette figyelembe a kormányzat (163/A/1996). Kifogásolta, hogy a háziorvosi körzethatárok módosítása esetén az új körzetbe automatikusan továbbítják a betegek törzskartonját és egyéb adatait, az információs önrendelkezés biztosítása nélkül (103/K/1999). A rendőrség nyomozásához olyan módon szeretett volna adatokat szerezni, hogy a hadkötelesek adatbázisából a pszichiátriai ok miatt alkalmatlanok személyes adatait igényelték volna. A biztos ellenezte ezt a fajta általános adatkérést, amire a rendőrségi törvény sem ad lehetőséget (848/K/2000). Az Ukrajnából hazaszállított utolsó magyar hadifogoly, Torma András személyiségi jogaira figyelmeztette az Országos Neurológiai és Pszichiátria Intézetet (585/K/2000). Állásfoglalást adott ki a munkaköri alkalmassági vizsgálatokkal kapcsolatban és kifogásolta az adatkezelésre vonatkozó jogszabályt is, amelyet a mai napig nem módosított az Egészségügyi Minisztérium (359/A/2001).

Dr. Péterfalvi Attila András: (2001. december 11. – 2007. december 11.)

1957-ben született Budapesten, középiskolát a Veres Pálné Gimnázium Angol tagozat, egyetem: Eötvös Loránd Tudományegyetem ÁJTK.

Felsőfokú végzettség: jogász, ELTE ÁJTK, cum laude fokozat
Szakvizsga: jogi szakvizsga, külkereskedelmi szakjogász ELTE Jogi Továbbképző
Nyelvismeret: Angol nyelv, társalgási szint (C típusú, középfokú állami nyelvvizsga)

Oktatási tevékenysége:
– Korábban Államigazgatási Főiskola, jelenleg Budapesti Corvinus Egyetem Közigazgatástudományi Karán (Budapest) nappali, esti, levelező és másoddiplomás szakokon
Oktatási terület:
civilisztika (polgári jog, polgári eljárásjog, családjog), adatvédelem, információszabadság

Beosztásai:
– főiskolai docens:

– 2006-ban tiszteletbeli egyetemi tanári címet kapott a Károli Gáspár Református Egyetemen
– 2008-ban címzetes egyetemi tanári kinevezést kapott a Pázmány Péter Katolikus Egyetemen
– Állampolgári jogok biztosa, hivatalvezető 2008-

Az adatvédelemhez kapcsolódó tevékenység:

Az Államigazgatási Főiskolán tudományos munkaként a személyiségi jogok és az adatvédelem összefüggéseit vizsgálta, ennek következtében a 80-as évek vége óta a Központi Statisztikai Hivatal (KSH) felkérése alapján részt vett az első (a rendszerváltás következtében beterjesztésre nem került) adatvédelmi törvény elkészítésében, véleményezésében.
NATO ösztöndíj, 1991-ben: Információszabadság – adatvédelem – személyiségi jogok címmel.
Az adatvédelmi biztos irodájának munkájában külső szakértőként 1996 óta vett részt. 2001. december 11-én az Országgyűlés hat évre megválasztott adatvédelmi biztosnak.

Dr. Péterfalvi Attila adatvédelmi biztosi tevékenysége során számos alkalommal foglalt állás a pozitív banki adóslista ellen, amely még akkor is aránytalanul sérti az állampolgárok adatvédelemhez fűződő jogait, ha látszólag önkéntes adatkezelésen alapul. Hivatalbeli működése során következetesen kiállt az okmánymásolás gyakorlata ellen. Sem a biztosítóknál (1069/A/2005), sem a bankoknál (1034/A/2006), sem pedig a telekommunikációs cégeknél (619/H/2004) nem tartotta jogszerűnek ezt a gyakorlatot. Ez az ötlet Franciaországból és Belgiumból érkezett hozzánk: ott az adatvédelmi biztos szerint támogatandó a személyazonosító igazolvány rámásolása minden olyan iratra, amelynél szükséges, hogy a címzett megbízható módon azonosítani tudja a levélírót. Állásfoglalást bocsátott ki arról, hogy a közlevéltárakban őrzött iratokon szereplő adatok között nem minden adat közérdekű, hanem egy részük a magánéletre vonatkozó személyes adat (1895/K/2006). Fellépett a kötelező számlaadást (és ezért a vevők személyes adatainak kényszer nyilvántartását is) elrendelő pénzügyminisztériumi rendelet ellen. Érvelését az Alkotmánybíróság is elfogadta.

Állásfoglalást adott ki a bírósági határozatok anonimizálásával kapcsolatos jogi felelősség kérdéséről (1944/K/2007). Ennek lényege, hogy a helytelenül, nem megfelelő körültekintéssel készült anonimizálás miatt a polgári jogi felelősséget vállalnia kell a közzé tevőknek. Állásfoglalást adott ki a történeti kutatás eredményeként feltárt személyes adatok nyilvánosságra hozásának jogszerűségéről (431/K/2005). Foglalkozott az MTV Rt. szerződéseinek nyilvánosságával (210/K/2005). Állásfoglalást adott ki arról, hogy az elektronikusan (e-mailben) érkező közérdekű adatkéréseknek is az adatvédelmi törvény szerint eleget kell tenni (1918/A/2004). Állásfoglalást adott ki a gázár-támogatás igényléséről szóló Kormányrendelettel kapcsolatban (2006. dec. 1.), amelyben bírálta a jogszabályt ugyanis az önkéntes adatkezelésként kezelte az igénylést, ugyanakkor számos kérdésről nem rendelkezett kielégítően. Bírálta azt a kormányzati tervet, amely a társadalombiztosítási és adóazonosító jelnek együttes tárolását rendelte volna el az egészségügyi pénztárak esetén (1730/K/2006).

Adatvédelmi biztosként foglalkozott az egészségügyi rendszerben előforduló adatkezelésekkel is. Fontos állásfoglalást adott ki a közgyógyellátással kapcsolatos adatkezelésről, amelyben kinyilvánította, hogy az önkormányzatok nem juthatnak hozzá személyes gyógyszerfogyasztási adatokhoz (1010/H/2006). Bírálta az anonim HIV ellenanyag szűrés rend-

szerét, amelynek során a szűrt páciensek TAJ számát rögzítik (2004. szept. 27.). Szót emelt a Baptista Szeretetszolgálat tűcsere programjában résztvevő önkéntesek rendőri igazoltatása ellen (909/K/2002), és azért mert a mentőszolgálat rendszeresen továbbította a kábítószer fogyasztó betegek személyes adatait a rendőrség számára. A halapenz.hu oldal működtetését sem tartotta jogszerűnek, mivel azon személyes adatokat hoztak nyilvánosságra megfelelő jogalap nélkül (2/H/2004). Ellenezte azt is, hogy a szexuális úton terjedő fertőző megbetegedések személyes adatait az OEP számára azonosítható módon továbbítsák (2005. nov. 15.) – ezt azonban az Egészségügy Minisztérium nem vette figyelembe. Állásfoglalást adott ki a háziorvosok részletes betegforgalmi jelentése miatt, és ellenzett számos 2006-ban újonnan bevezetett adatküldést az OEP számára (1301/A/2006) – ezt az állásfoglalást sem vette figyelembe az Egészségügyi Minisztérium. Állásfoglalást adott ki a háziorvosi praxis jogutódlása esetén a személyes egészségügyi adatok sorsáról. Eszerint az új háziorvos alaphelyzetben meg kell kapja elődjétől az összes egészségügyi adatot, a páciensek ellátása érdekében (1799/A/2004). A háziorvos nem kezelheti a páciense fényképét személyazonosítás céljából (1748/K/2006). Állásfoglalást adott ki a kórházi azonosító karszalagok ügyében és a személyes adatokon végzett orvosi kutatások jogszerű végzésével kapcsolatban (2006. máj. 19.). Az Alkotmánybírósághoz fordult a vizitdíj számlák adatkezelése ügyében, de mivel időközben a vizitdíj megszűnt, az AB az eljárást 2010 októberében megszüntette (1213/B/2006. számú határozat).

Dr. Jóri András: (2008. szeptember 29. –

1972-ben Szegeden született.

Végzettségek:
Felsőfokú végzettség: jogász, ELTE ÁJTK, 1997
Jogi szakvizsga: 2000
PhD abszolutórium: Pécsi Egyetem, ÁJTK, Jogi Informatika doktori program, 2004 (a doktori eljárás folyamatban)
Rendszerinformatikus (rendszergazda) OKJ szerinti felsőfokú szakképesítés, ELTE TTK Informatikai Tanszékcsoport, 1999.

Nyelvek:
Angol (TOEFL 630, 1997; állami középfokú "C", 1988)
Német (Goethe Institut ZD "sehr gut", 2006; állami középfokú "C", 2006)

Szakmai tapasztalatok:
Ügyvéd: 2001–2008
Szakterület: adatvédelmi jog, informatikai jog, gazdasági és társasági jog
Internetszolgáltatók Tanácsa, a Jogi Tanácsadó Testület tagja 2000-2008
Döntések hozatala a .hu nemzeti fődomain adminisztrációját végző ISZT mellett működő, felkért független szakértőkből álló bizottság tagjaként a domain nevek választhatóságával kapcsolatos vitás kérdésekben; Infomediátor iroda, Regisztrációs döntnök, 2006-2008
Adatvédelmi szakértő, Országgyűlési Biztosok Hivatala, Adatvédelmi Biztos Irodája, 1997–2000

Oktatási és tudományos tevékenység:
Előadó, PTE ÁJK infokommunikációs szakjogász képzés („Adatvédelem a gyakorlatban”), 2006-
A programbizottság elnöke, Adatvédelem és adatbiztonság 2006 konferencia
A programbizottság elnöke, Adatvédelem és adatbiztonság 2005 konferencia

Szerkesztő, Infokommunikáció és Jog, 2004-
Szerkesztő, http://www.jogiforum.hu/adatvedelem portál, 2004-
Szerkesztő, http://www.dataprotection.eu jogösszehasonlító portál, 2007-

Publikációk:
Könyv: Adatvédelmi kézikönyv – Elmélet, történet, kommentár, Osiris, 2005
(A bevezetőt bírálta dr. Majtényi László, az ajánlást írta dr. Péterfalvi Attila)

Könyvfejezetek:
Magánszféra és nyilvánosság a digitális korban, in: Magyarország Médiakönyve 2002, Enamiké, Budapest, 2002.
Az elektronikus információszabadság lehetőségei Magyarországon, in: Magyarország Médiakönyve 2003.
A nyilvánosság határai: a személyes adat, a közérdekű adat és a közérdekből nyilvános adat fogalma az adatvédelmi biztos és az Alkotmánybíróság gyakorlatában, in: Tízéves az Adatvédelmi Biztos Irodája, Adatvédelmi Biztos Irodája, Budapest, 2006.
Az adatvédelmi szabályozás generációi és jövője, in: Az ombudsman intézménye és az emberi jogok védelme Magyarországon, Országgyűlési Biztosok Hivatala, Budapest, 2008.
Az Alkotmány 59. §-ának kommentárja, in: Jakab András (szerk.): Az Alkotmány kommentárja, Századvég, 2008.

Szakmai folyóiratban megjelent cikkek, fordítások :
Adatvédelem és információszabadság (válasz a szerkesztők körkérdésére), Fundamentum, 2004/4
Vitás kérdések az adatvédelmi törvény értelmezése körül, Infokommunikáció és Jog, 2005/5 (társszerző: Bártfai Zsolt)
Az adatvédelmi törvény újabb módosításáról, Infokommunikáció és Jog, 2005/6,
Targetált hirdetések, felhasználói profilok képzése és adatvédelem – Az elektronikus kereskedelemről szóló törvény adatvédelmi rendelkezéseiről, Infokommunikáció és Jog, 2006/4
An Outline of the History of Data Protection, ICT and Law, 2008/2

Egyéb publikációi:
Adatvédelmi „legjobb gyakorlat” kialakítása az elektronikus közigazgatásban, PTE Állam- és Jogtudományi Kar, Informatikai Jogi Műhely, 2001 (társszerzők: Balogh Zsolt György, Polyák Gábor)
Elektronikus információszabadság és állami adatvagyon – A 2003/98/EK irányelv átültetése, Jogi Fórum (http://www.jogiforum.hu), 2006. április 25.
Az információszabadság elektronikus kézikönyve (elektronikus tananyag), Jogászoknak Kft., 2008 (társszerző: Szabó Máté Dániel)

Ösztöndíjak:
Office of the Data Protection Commissioner, Wilmslow, Cheshire, UK, 2000 (PHARE ösztöndíj):
Tanulmány készítése az Igazságügyi Minisztérium számára a brit adatvédelmi jogról és a hitelinformációs rendszerek nagy-britanniai szabályozásáról

Universität Wien, 2004 (Eötvös-ösztöndíj): A német nyelvű jogirodalom kutatása az Adatvédelmi kézikönyv elméleti-történeti fejezetének elkészítéséhez.

Dr. Jóri András adatvédelmi biztosi tevékenységének első napjaiban közleményt adott ki az ún. pozitív banki adóslista ügyében. Az előző adatvédelmi biztosok hasonló nyilatko-

zataival megegyezően úgy foglalt állást, hogy ilyen lista létrehozása üzleti érdekből aránytalanul korlátozná az állampolgárok adatvédelemhez fűződő jogait (2008. okt. 30.). Mint adatvédelmi biztos ajánlást dolgozott ki a bankok számára a pénzbefizetések során alkalmazható személyazonosítási módokról (2009. aug. 5.). Ennek lényege, hogy 1000 Eurónál kisebb befizetés esetén nincs szükség a személyazonosító okmányok számának rögzítésére. Állásfoglalást adott ki a munkahelyek gépjárműveibe szerelt GPS nyomkövetőkkel kapcsolatban, amelyben leszögezte, hogy jogszabályi felhatalmazás hiányában a munkavállaló önkéntes hozzájárulása lehet az adatkezelés jogalapja (415/K/2009). Állásfoglalást adott ki a munkahelyi ujjlenyomat alapú biometrikus beléptető rendszerekkel kapcsolatban, amelynek a lényege az volt, hogy jogszabályi felhatalmazás nélkül a munkáltató nem képezhet olyan adatbázist, amely a dolgozók adatai mellett az ujjlenyomatuk képét vagy hash kódját is tartalmazza (110/K/2009). Az azonban megengedhető, hogy egy hash kódot tartalmazó kártyát adjanak a dolgozóknak, a rendszer pedig a kártyán lévő és a leolvasott adatok alapján dönt a belépés engedélyezéséről. Állásfoglalásában megtiltotta a munkahelyeken a munkavállalók poligráfos (hazugságvizsgáló eszköz) vizsgálatát (369/K/2009).

Az önkormányzati segélyben részesülő, de a segélyt át nem vevő állampolgárok személyes adatait nyilvánosságra hozó hódmezővásárhelyi önkormányzat ügyében úgy foglalt állást, hogy a személyes adatok közzé tételének nincs meg a jogszabályi alapja, ezért jogellenes (3241/2010/K). Nagy sajtóvisszhangja volt az adatvédelmi biztos ajánlásának, amely szerint az egyetemi rektorok fizetése közérdekű adat és nyilvánosságra kellene hozni (2250/H/2009). A BKV járművein történő kamerás megfigyelésről szólva úgy foglalt állást, hogy egyelőre törvényi felhatalmazás hiányában nem lehetséges az utastér kamerás megfigyelése, amelynek során az adatok rögzítésre kerülnek (1781/K/2009). A levéltárak által alkalmazott másolási díjszabás ügyében megállapította, hogy a levéltári anyagok a közérdekű adatok közé tartoznak, ezért az adatvédelmi törvény szerint a másolat készítés során kizárólag a másolás közvetlen költsége számolható el jogosan, nyereség nélkül (1121/2010/K).

Az egészségügyi intézmények ellátó helyiségeiben felszerelendő kamerák alkalmazását is jogellenesnek és az emberi méltóságot sértőnek találta (2243/K/2009). Az egyetem nem kérheti a vizsgahalasztási kérelemhez a beteg hallgató BNO kódját (522/2010/K). A H1N1 influenza védőoltás esetén a munkáltató kórház nem kérheti, hogy a munkavállalók nyilatkozzanak az oltás elfogadásáról (200/2010/P). A megszűnt kórházakból elszállított dokumentáció ügyében megállapította, hogy a Schöpf-Merei Kórház elszállított dokumentáció nem állnak a páciensek rendelkezésére, ezért sérül az egészséghez való joguk (573/2010/K). A TASZ kérésére kibocsátott állásfoglalásában (1504/2010/K) kinyilvánította, hogy az Országos Epidemológiai Központ számára jogellenesen kerül továbbításra a HIV pozitív személyek TAJ száma.

Ellenőrző kérdések

1. Milyen európai uniós kötelezettsége van a tagállamoknak az adatvédelem nemzeti intézményrendszerét illetően?

2. Mely törvény rendelkezik az adatvédelmi biztos választásáról és működéséről?

3. Az adatvédelmi törvény szabályozza-e teljes mértékben az adatvédelmi biztos működését?

4. Milyen tevékenységei vannak az adatvédelmi biztosnak?

5. Milyen viszonyban áll egymással az adatvédelmi biztos eljárása és a bírósági jogorvoslat?

6. Milyen beavatkozási joga van az adatvédelmi biztosnak, ha rendellenességet tapasztal?

7. Sorolja fel az eddigi magyar adatvédelmi biztosokat!

8. Mutassa be Dr. Majtényi László adatvédelmi biztosi tevékenységét!

9. Méltassa Dr. Péterfalvi Attila adatvédelmi biztosi tevékenységét!

10. Mutassa be Dr. Jóri András, jelenlegi adatvédelmi biztos eddigi tevékenységét!

További szakirodalom

[1] Dr. Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve, Complex Kiadó, 2009.
[2] Eckstein, S. (szerk.): *Manual for Research Ethics Committees*, King's College, ISBN: 0521810043, (2003).
[3] Matti Häyry, Ruth Chadwick, Vilhjálmur Árnason és Gardar Árnason: The Ethics and Governance of Human Genetic Databases, Cambridge University Press, 2007.
[4] Dr. Jóri András: *Adatvédelmi kézikönyv*, ISBN: 963 3897 351, Osiris Kiadó, 2005.
[5] Dr. Jóri András, Dr. Hegedűs Bulcsú, Dr. Kerekes Zsuzsanna (szerk.): *Adatvédelem és információszabadság a gyakorlatban*, Complex Kiadó, Budapest, 2010.
[6] Dr. Ködmön István (szerk.): *Hétpecsétes történetek, információbiztonság az ISO 27001 tükrében*, Hétpecsét Információbiztonsági Egyesület, Budapest, 2008.
[7] Susan Loepp, W. K. Wooters: *Protecting Information, from Classical Error Correction to Quantum Cryptography*, Cambridge University Press, 2006
[8] Lowrance, W. W.: *Privacy and the Secondary Use of Data in Health Research*, 2002, Nuffield Trust, white paper, pp. 66-67.
Letölthető: http://www.nuffieldtrust.org.uk/ecomm/files/161202learning.pdf
[9] Dr. Majtényi László: *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága*, ISBN: 9632247604, 2006
[10] Sándor, Judit (szerk.): *Society and Genetic Information*, Central European University Press, 2003.
[11] Schaar, Peter: *Das Ende der Privatsphäre, der Weg in die Überwachungsgesellschaft*, paperback, C. Bertelsmann, 2007.
[12] Schaar, Peter: *Datenschutz im Internet. Die Grundlagen*, paperback, C. H. Beck, 2002.
[13] Dr. Székely Iván, Dr. Szabó Máté Dániel (szerkesztők): *Szabad adatok, védett adatok*, BME GTK Információ és Tudásmenedzsment Tanszék, 2005.

Tárgymutató

Sz

T

U,Ú

V

W