DRINÓCZI TÍMEA – KOCSIS MIKLÓS – ZELLER JUDIT

A SZEMÉLYES ADATOK VÉDELME ÉS A BIOMETRIKUS AZONOSÍTÓ SZEREPE A SZUPRANACIONÁLIS SZABÁLYOZÁS TÜKRÉBEN

A) A biometrikus azonosítás

I. A biometrikus azonosítók fogalma, jellegzetességei

Általános definíció nyomán *„[a] biometrikus azonosító az ember olyan egyedi, mérhető jellegzetessége, amely alkalmas arra, hogy a személyazonosságot felismerje, illetve igazolja*”.[80] Ez a mérhető jellegzetesség lehet fiziológiai, mint például a szem (írisz), az arc, az ujjnyomat a kézgeometria, illetve viselkedéses, mint például a hang,[81] az aláírás és a gépelési ritmus (billentyűleütési szekvencia). Fontos ismérv, hogy a biometrikus vonást a felismerő rendszer gyorsan és automatikusan képes legyen felismerni és azonosítani.[82]

A számos, azonosításra használt biometrikus jellemző közül a legnépszerűbbek az arckép,[83] az íriszkép[84] és az ujjnyomat.[85] Emellett egyes biometrikus azonosító rendszerek retinavizsgálaton,[86] hangazonosításon, illetve az aláírás[87] vagy a tenyérgeometria[88]

---

[80] Huopio, S.: Biometric Identification. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm (2007. 12. 10.)

[81] Szigorúan véve a hang is fiziológiai vonás, amennyiben kizárólag a személy hangmagaságát vesszük figyelembe. A hangazonosítás azonban leginkább annak tanulmányozásán alapul, hogy a személy hogyan beszél, amely viszont már viselkedéses jegyként fogható fel.

[82] Huopio: i. m.

[83] Az arcazonosítási módszerek az arc egyedi formáját, valamint az arcvonások sajátos mintázatát és elhelyezkedését elemzik. Az arc természetes biometrikus aonosító, mivel kulcsösszetevője annak a módnak is, amellyel mi emberek számon tartjuk és azonosítjuk egymást. Az arcazonosítás nagyon összetett és leginkább szoftver-alapú technológia. Az emberi arccal kapcsolatban felmerülő probléma, hogy az emberek az idő előrehaladtával változnak; ráncosak lesznek, szemüveget vagy szakállt viselnek, és a felj elhelyezkedése is befolyásolhatja az azonosítás megvalósítását. A pontosság növelése és a változások követése érdekében szükséges a gépesítés folyamatos fejlesztése.
http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm (2007. 12. 10.)

[84] Az írisz a szem belső szerve, amely a pupilla körüli színes karikaként jelenik meg. Minden írisz egyedi felépítéssel bír, olyan jelleget jelent, amely stabil és az élet folyamán nem változik. Az írisz szorosan kapcsolódik az agyhoz, és az első szervek közé tartozik, amelyek a halál után elsorvadnak. Ennek köszönhetően a halott szemének újjáteremtése vagy jogosulatlan felhasználása nagyon bonyolult. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/ biometric.htm (2007. 12. 10.)

[85] Az ujjnyomat vizsgálata napjaink egyik legeredményesebb biometrikus azonosító technológiája. Széleskörben elfogadott, hogy az emberi ujjnyomat egyedi, még egyfetéjű ikrek esetében is van eltérés. Az ujjnyomatok szisztematikus osztáloyzása az 1800-as években kezdődött, és folyamatosan fejlődött a kriminalisztika területén. Hátránya azonban, hogy az emberek az ujjnyomatvételt gyakran a bűnelkövetők kezelésével azonosítják. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm (2007. 12. 10.)

[86] A retina az erek rétege a szem hátsó részén. Hasonlóan az íriszhez, a retina is egyedi mintázatot alkot, és hamar elkezd bomlani a halál beállta után. A retinális szkenneklésen alapuló azonosítást – az íriszvizsgálat mellett – a biometrikus azonosítás egyik legpontosabb módszernek tartják. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/ biometric.htm (2007. 12. 10.)

[87] Az aláírás az egyik legáltalánosabb módszer az egyén személyazonosságának igazolására. Hagyományos alkalmazásánál az aláírás a toll nyoma a papíron. Digitalizált formában az aláírás statikus elemei azonban nem

elemzésén alapulnak. Jelenleg még fejlesztés alatt áll az a rendszer, amely a testszag kémiai összetételének felismerésére képes. A kutatások legnagyobb reményt a DNS-en alapuló azonosításhoz fűznek, ezt tekintik a jövő „vezető biometrikus azonosítójának". Jelenleg azonban a DNS-elemzés a leggyorsabb esetben is legalább tíz percet, és minden esetben emberi segítséget igényel, ezért egyelőre nem felel meg a biometrikus azonosítás követelményeinek, amelyek szerint a gyorsaság és az automatizáltság nélkülözhetetlen. Mindemellett a DNS-minta megszerzésének módja – pl. a vérvétel vagy a nyálminta – különösen jelentős beavatkozást jelent más biometrikus azonosítók gyűjtési módjaihoz képest. Amennyiben ezektől a hátrányoktól eltekintünk, a DNS valóban nagy lehetőségeket rejt az azonosítás terén.[89] Az emberi test meghatározhatatlan számú olyan részlettel rendelkezik, amelyek biometrikus azonosításra használhatók. A leginkább észrevehető, látható és hallható vonások mellett folyik az egyre újabb és újabb biometrikus azonosítók kiaknázása. Példaként említhető az a kutatás, amely az egyén *szerveiből sugárzott vibráció* alapján kívánja az egyedi azonosítást megvalósítani.[90]

Az azonosítás biometrikus adatokon alapuló módszere számos előnyt kínál a hagyományos megoldásokkal – igazolványok (illetve különféle magunknál tartható tárgyak, ún. „zsetonok"), illetve a PIN-kódok (belépési jelszavak) alkalmazásával – szemben. Egyrészt az azonosítandó egyénnek fizikai értelembe jelen kell lennie az azonosítási folyamat során, másrészt az azonosításhoz nincs szükség jelszó megjegyzésére vagy „zsetonok" bemutatására.[91] A számítógépek és az internet egyre mélyebb integrálódása

elégségesek az egyediség biztosítására. Az aláírási adatot ezért speciális táblán vagy tollal rögzítik. E technikák akusztikus sugárzásként került kifejlesztésre, amely módszer a hangot vizsgálja, amelyet a toll kelt a papíron. Az aláírás viselkedéses jellege miatt több aláírás is szükséges ahhoz, hogy a rendszer egyedi aláírás-profilt tudjon kialakítani az aláírás jellegzetességeiből.
http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm (2007. 12. 10.)

[88] A kézgeometria mérésénél a kézről háromdimenziós kép készül, amelyen megmérik az ujjak és az ízületek formáját és hosszát. Ez a módszer nem biztosít jelentős pontosságot, de alkalmas az azonosításra és gyors. http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/ biometric.htm (2007. 12. 10.)

[89] A DNS-elemzés nagyon nagy pontosságú: a statisztikák szerint egy a hatmilliárdhoz az esélye annak, hogy két embernek azonos DNS-mintázata legyen (kivételt képeznek persze az egypetéjű ikrek). A DNS megfelel a biometrikus azonosítókkal szemben támasztott valamennyi követelménynek: jelen van minden emberben (univerzális), és az ikrek kivételével a legjobban elhatárolható vonás. A DNS nem változik az egyén élete során, állandósága ezért vitathatatlan. A DNS-teszteket bonyolult hamisítani, amennyiben a mintavétel ellenőrzött. A DNS legfőbb problémája, hogy az egyén genetikai vonásaival és egészségügyi állapotával kapcsolatos különleges adatokat is magában hordozhat, ezért a DNS-sel való visszaélés információt fedhet fel az örökletes vonásokkal, illetve az orvosi rendellenességekkel összefüggésben. Az általában alkalmazott DNS-profil azonban csupán egy számsor, amely egyáltalán nem hordoz információs, illetve semleges. Szem előtt tartandó, hogy a DNS-nek vannak ún. nemkódoló régiói, amely körülbelül a DNS 10%-át alkotják, és nem hordoznak különleges információt. A DNS-részletek kiválasztása az igazságügyi szakértők által úgy történik, hogy azok lehetőség szerint nemkódoló, vagyis semleges részek legyenek; olyanok, amelyek a gének között vagy azoktól távol helyezkednek el. Ezáltal a DNS-részek nem hozhatók kapcsolatba egyes genetikai betegségekkel. Mindezek ellenére a DNS-ből megállapítható a rassz, illetve a felmenők származása. Vö. European Commission: Biometrics at the Frontiers: Assessing the Impact on Society. Report of the Joint Research Centre (DG JRC) Institute for Prospective Technological Studies. European Communities 2005. http://ftp.jrc.es/pub/EURdoc/eur21585en.pdf (2007. 12. 10.)

[90] http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/12biometric/biometric.htm (2007. 12. 10.)

[91] Jelenleg az egyén – azt az esetet kivéve, amikor a személyazonosságot megbízható harmadik fél személyesen tanúsítja – kizárólag sajátos, ún. *„zsetonok"* segítségével azonosítható. Ezek az igazolványok, amelyek valójában harmadik fél esküjének eprezentációi, alapvetően kétfélék lehetnek: (i) *ismereti zsetonok*, mint a jelszavak, PIN-kódok vagy a személyes adatok ismerete (pl. az anya leánykori neve) vagy (ii) *fizikai zsetonok*, mint igazolványok, útlevél, csipkártya vagy a hagyományos kulcs. A zsetonjellegű azonosítók rendelkeznek bizonyos előnyökkel a biometrikus azonosítókkal szemben. A csalók által használt zsetonok téves jóváhagyása csökkenthető a zseton összetettségének növelésével. Az elvesztés esetén a zseton kicserélhető vagy újra kiállítható, míg a biometrikus azonosító nem. A biometrikus azonosítók előnye a zsetonokkal szemben, hogy ezek nem veszíthetők el, nem

mindennapi életünkbe szükségessé teszi a személyes adatok szigorú védelmét. A PIN-kódok teljes vagy részleges helyettesítésével a biometrikus technikák megelőzhetik a jogosulatlan hozzáférést az ATM automatákhoz, a mobiltelefonokhoz vagy számítógépes hálózatokhoz. A biometrikus azonosítókkal szemben a PIN-kódok vagy jelszavak mások számára hozzáférhetővé válhatnak, illetve birtokosul elfelejtheti őket, a „zsetonok" hamisíthatók, ellophatók vagy elveszíthetők. Összefoglalva tehát a biometrikus rendszerek kifejlesztése fokozhatja a biztonságot, és csökkentheti a csalások mértékét.

II. A biometrikus azonosítók alkalmazásának területei

A biometrikus azonosításon alapuló rendszerek, különösen az ujjnyomat-felismerés már régóta széles körben alkalmazott a büntetőeljárásban. Emellett azonban egyre gyakrabban kerül sor biometrikus adatok felhasználására a közigazgatásban, valamint a magánszférában egyaránt. A beléptető rendszerek, a számítógépes bejelentkezés, a szociális szolgáltatások igénybe vétele, valamint az államhatárok átlépésére jogosító, illetve a nemzeti személyazonosító igazolványokban történő feltüntetés csak néhány példa a közigazgatási és magáncélú felhasználásra. A biometrikus adatok alkalmasak lehetnek arra, hogy azonosítsák a vevőt telefonos vagy internetes tranzakciók során (az elektronikus kereskedelemben vagy elektronikus bankszámlakezelés esetén), a gépkocsikban helyettesíthetik az indítókulcsot.

Mindent összevetve a biometrikus azonosítók lehetőséget adnak az egyre növekvő biztonsági kockázatok (terrorizmus, globális kihívások) leküzdésére. A biztonság megteremtése mellett azonban fontos, hogy a biometrikus adatok alkalmazása akár a köz- akár a magánszférában olyan, pontosan meghatározott jogi keretek között menjen végbe, amelyek megelőzik a visszaéléseket, valamint minden esetben biztosítják az emberi jogok tiszteletben tartását.

B) A biometrikus azonosítókkal kapcsolatos nemzetközi és szupranacionális szabályozás

I. Nemzetközi dokumentumok

1. Adatvédelmi háttér

A nemzetközi szerződések körében mindmáig (2008-ig) nem született olyan dokumentum, amely kifejezetten a biometrikus adatok védelmével foglalkozna, így a biometrikus adatok esetében is az általános adatvédelmi szabályokhoz és elvekhez indokolt visszanyúlni. A Magyarországon kihirdetett nemzetközi egyezmények közül több is a magánszféra védelmének körébe ágyazva, implicit módon rögzíti a személyes adatok védelmét, így a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának[92] 17. cikke[93]

adhatók kölcsön, illetve nem felejthetők el. A zsetonalapú rendszereknek azt is igazolniuk kell, hogy a zsetont bemutató személy annak jogos használója is, nem pedig illetéktelen személy, aki a zseton birtokába jutott. Óvatosan alkalmazva a biometrikus azonosítók a zsetonokkal kombinálva enyhíthetik az azonosító zsetonokkal való visszaélést. Vö. http://www.eff.org/wp/biometrics-whos-watching-you (2007. 12. 10.)

[92] Magyarországon kihirdette az 1976. évi 8. tvr.

[93] „*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*"

vagy az Emberi Jogok Európai Egyezményének[94] (EJEE) 8. cikke.[95] Az Emberi Jogok Európai Bíróságának (EJEB) töretlen gyakorlatából egyértelműen kitűnik, hogy a személyes adatok védelme – így a biometrikus adatok védelme is – a magánélet szabadságának területére tartozik.[96]

Az adatvédelem nemzetközi dokumentumai között említhető az Európa Tanács 1981. január 28. napján kelt Egyezménye az egyének védelméről a személyes adatok gépi feldolgozása során (Adatvédelmi Egyezmény),[97] valamint az Adatvédelmi Egyezmény 2001. november 8-án kelt Kiegészítő Jegyzőkönyve a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról (Kiegészítő Jegyzőkönyv).[98] Az Adatvédelmi Egyezmény célja, hogy a magánélethez való jog tiszteletben tartását elősegítse a személyes adatok automatizált feldolgozása során is. Kizárólag tisztességesen és törvényesen szerzett, pontos és időszerű személyes adatok gépi segítséggel történő kezelését teszi lehetővé, csak törvényben meghatározott célból és a cél elérésével arányos mértékben.[99] Az adatalany joga, hogy tudomást szerezzen a vele kapcsolatos adatfeldolgozásról, valamint szükség esetén adatainak kijavítását vagy törlését kezdeményezhesse, amennyiben az adatkezelés nem a rögzített elvek szerint történik.[100] A különleges (faji eredetre, politikai irányultságra, vallási vagy más meggyőződésre vonatkozó, illetve az egészségi állapotot vagy a szexuális életet érintő) adatok gépi feldolgozása csak akkor megengedett, ha a belső jog ehhez megfelelő biztosítékokat nyújt.[101] Tekintettel arra, hogy egyes biometrikus azonosítók besorolhatók a különleges adatnak minősülő egészségügyi adatok körébe, az Adatvédelmi Egyezmény releváns a biometrikus adatok szabályozása szempontjából. Az Adatvédelmi Egyezmény kitér az országhatárokon átívelő adatáramlásra is. A Kiegészítő Jegyzőkönyv az adatvédelem intézményi garanciájaként előírja független felügyelő hatóságok felállításának kötelezettségét valamennyi részes állam számára; ezek a hatóságok az egyéni panaszok elbírálására jogosultak, döntésük pedig bíróság előtt megtámadható.[102] Kimondja továbbá, hogy az Adatvédelmi Egyezményben nem részes államok joghatósága alatt állók számára csak akkor továbbíthatók személyes adatok, amennyiben ott is biztosított a megfelelő védelmi szint.[103]

Tekintettel a már említett kapcsolatra a biometrikus adatok és az egészségügyi adatok között, megemlítendők azok a nemzetközi források is, amelyek az egyén egészségügyi személyes adatait védik. Ilyen forrásnak tekinthető az Európa Tanács égisze alatt született Biomedicina Egyezmény.[104] Ennek preambuluma kimondja, hogy azt az Adatvédelmi Egyezményre tekintettel alkották meg, 10. cikke pedig deklarálja, hogy mindenkinek joga van magánéletének tiszteletben tartására az egészségével kapcsolatos adataival összefüggésben, mindenkinek joga van továbbá megismerni az egészségével

[94] Magyarországon kihirdette az 1993. évi XXXI. törvény
[95] „Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák."
[96] Vö. például a Leander kontra Svédország üggyel (EJEB 1987. március 26-i ítélet).
[97] Magyarországon kihirdette az 1998. évi VI. törvény
[98] Magyarországon kihirdette a 2005. évi LIII. törvény
[99] Adatvédelmi Egyezmény 5. cikk
[100] Adatvédelmi Egyezmény 8. cikk
[101] Adatvédelmi Egyezmény 6. cikk
[102] Kiegészítő Jegyzőkönyv 1. cikk
[103] Kiegészítő Jegyzőkönyv 2. cikk
[104] 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, Magyarországon kihirdette a 2002. évi VI. törvény.

kapcsolatosan összegyűjtött valamennyi adatot. E jogok korlátozása csak kivételes esetben, a beteg érdekében és törvény által történhet.

2. A biometrikus azonosítók alkalmazása

A biometrikus adatok felhasználásának elsődleges indoka kezdettől fogva a terrorizmus elleni harc, alkalmazásának fő területe pedig a személyek azonosítása, valamint ezzel összefüggésben az egyének szabad mozgásának ellenőrzése.[105] Biometrikus adatok tehát tipikusan az úti okmányokban (esetleg más, személyazonosítás célját szolgáló hivatalos iratokban) és vízumokban szerepelhetnek, a felhasználás legfőbb célja pedig a bűnmegelőzés és a bűnüldözés.

A biometrikus adatok alkalmazásának megindulása elsődlegesen az Egyesült Államok nyomásának volt köszönhető, amely a 2001. szeptember 11-i terrortámadás után erősödött fel. A biometrikus adatok felhasználásának területén jellemző a vonatkozó nemzetközi szabályozás „soft law" jellege, illetve hiányos legitimációja. Nemzetközi szinten a biometrikus adatok alapján történő azonosítás általános standardjainak megállapítását az ENSZ égisze alatt működő Nemzetközi Polgári Repülési Szervezet (ICAO) végezte el. Ez a szervezet alapító okmányának tanúsága szerint nem rendelkezik felhatalmazással arra vonatkozóan, hogy a részes államok számára kötelező erejű dokumentumokat bocsásson ki,[106] mégis mintegy 50 éve felelősséget vállal az úti okmányok standardjainak megállapításáért. Mivel majdnem minden részes állam elfogadta az ICAO által kiadott előírásokat, a szervezet e jogterület szinte kizárólagos befolyásoló tényezőjét jelenti.[107]

2003-ban[108] kerültek megállapításra a géppel olvasható úti okmányok új standardjai, bevezetendő a biometrikus azonosítás módszerét. Elsődleges biometrikus azonosítóként az ICAO az arcot jelölte meg, amelynek mását nagyfelbontású, digitalizált kép formájában, ún. kapcsolat nélküli (vagyis központi adatbázissal összeköttetésben nem lévő) chipen kell tárolni. Ez elősegíti, hogy valamennyi országban megtörténhessen az azonosítás, és államok közötti azonosítási átjárhatóság, az ún. interoperbilitás is megvalósuljon.[109] Az ICAO-val szemben felvetődő kritika, hogy a szervezet nem áll demokratikus irányítás és ellenőrzés alatt. Igaz, hogy az ICAO közgyűlésében valamennyi részes állam rendelkezik szavazati joggal, ám tanácsa csupán 33 tagból áll, akiket úgy választanak, hogy közöttük a légi szállításban legfontosabb szerepet betöltő, a polgári repülés lehetőségeinek előmozdításához a legnagyobb támogatást nyújtó, valamint a világ földrajzi egységeit megfelelően képviselni képes államok kielégítő módon reprezentáltak legyenek.[110] Mindez azt jelenti, hogy az az állam, amely több anyagi, illetve humán

[105] Az Európai Unió Tanácsa a 2004. november 4-5-én elfogadott Hágai Program prioritásai alapvetően az Unión belüli szabadság, biztonság és jog megerősítését tűzik ki célul. Külön prioritást testesít meg a terrorizmus elleni harc, amelynek keretében említésre kerül a biometrikus azonosítók alkalmazása. Vö. The Hague Programme: ten priorities for the next five years. http://europa.eu/scadplus/leg/en/lvb/l16002.htm (2007. 12. 03.)

[106] Egyezmény a Nemzetközi Polgári Repülésről (a továbbiakban: Chicagói Egyezmény), http://www.icao.int/icaonet/dcs/7300.html. (2007. 12. 10.)

[107] Dr. Gerrit Hornung: The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards. Script-ed. Volume 4, Issue 3, September 2007. 254. o.

[108] Vö. az ICAO DOC 9303 számú dokumentumával

[109] European Commission: Biometrics at the Frontiers: Assessing the Impact on Society. Report of the Joint Research Centre (DG JRC) Institute for Prospective Technological Studies, European Communities 2005. http://ftp.jrc.es/pub/EURdoc/eur21585en.pdf (2007. 10. 25.)

[110] Chicagói Egyezmény 50. (b) cikk

erőforrást szolgáltat az ICAO számára, nagyobb befolyást gyakorolhat az egyes standardok, illetve más előírások kialakítására.[111]

II. Szupranacionális szabályozás

1. Adatvédelmi háttér

Az Európai Unió alapjogvédelme a személyes adatokkal kapcsolatban az Unió Alapjogi Chartájában (Charta), valamint ennek nyomán az Európai Unió Alkotmányában (EUA) került megfogalmazásra. A Charta 8. cikke alapján mindenkinek joga van a rá vonatkozó személyes adatok védelméhez, ezeket az adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett hozzájárulása alapján vagy törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van továbbá ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni. A személyes adatok védelméhez való jog uniós sorsának nyomon követéséből nem hagyható ki a Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (az ún. Reformszerződés), amelynek aláírására 2007. december 13-án került sor. A Reformszerződés fontos eleme, hogy az Alapjogi Chartát beemeli a jogilag kötelező erejű dokumentumok közé. A Reformszerződés az Európai Unióról szóló Szerződés 6. cikkét úgy módosítja, hogy az Unió elismeri az Alapjogi Chartában foglalt jogokat, szabadságokat és elveket, a Chartát pedig jogilag a Szerződésekkel azonos értékűvé teszi.[112] Ezzel nyilvánvalóan a személyes adatok védelméhez fűződő jog is az Európai Unió által kötelezően elismerendő és védendő jogok közé tartozik majd, amennyiben a tagállamok általi ratifikálási folyamat sikerrel jár.

Az Európai Unió biometrikus adatokra vonatkozó szabályozásának áttekintése előtt szükséges utalni az Unió adatvédelmi háttérjogszabályát jelentő 95/46/EK irányelvre (Adatvédelmi Irányelv). Az Adatvédelmi Irányelv preambuluma szerint elsődlegesnek tekinti a személyek alapvető jogainak és szabadságainak, különösen a magánélet szabadságának védelmét, tekintettel van továbbá arra, hogy a Közösség gazdasági és társadalmi tevékenysége egyre szélesebbé válik, így egyre gyakrabban kerül sor személyes adatok feldolgozására, amelyet ráadásul még az informatikai-technikai fejlődés is egyre könnyebbé és gördülékenyebbé tesz. A személyes adatok „veszélyeztetettségének" e tendenciáját erősíti, hogy várhatóan az állami adatfeldolgozás mellett a magánszféra általi adatfeldolgozás is szélesebb körben érvényesül majd. A tudományos és műszaki együttműködés keretében pedig az Unió olyan információs hálózatokat tervez létrehozni, amelyek megkönnyítik a személyes adatok határokon át történő áramlását. Mindezeket figyelembe véve leszögezhető, hogy az Adatvédelmi Irányelv a jövőbeni integrációs és technikai kihívásokra tekintettel került megalkotásra, amelyek azonos adatvédelmi standardokat kívánnak meg valamennyi tagállamtól.

Az Adatvédelmi Irányelv alkalmazandó a személyes adatok valamennyi, egészben vagy részben automatizált feldolgozására,[113] így a biometrikus adatok feldolgozására is. Az Irányelv meghatározza az adatkezelés alapvető elveit: a törvényesség és a célhoz kötöttség elvét, továbbá az adatok megfelelő minőségének követelményét, végül az adattárolás

[111] Hornung: i. m. 254. o.
[112] Vö. a Reformszerződés tervezetével. http://www.consilium.europa.eu/uedocs/cmsUpload/cg00001-re01.hu07.pdf (2007. 10. 25.)
[113] Adatvédelmi Irányelv 3. cikk (1) bek.

időbeli korlátozásának szabályát.[114] Személyes adatok kezelése alapvetően az érintett egyértelmű hozzájárulása mellett történhet, ezen kívül olyan esetekben, amelyben az adatkezelés az érintett érdekében történik vagy az adatfeldolgozó hivatali hatáskörével, illetve közfeladat-ellátásával, illetve harmadik fél jogszerű érdekének érvényesítésével kapcsolatos.[115] Az Irányelv külön rendelkezik a különleges adatok kezeléséről,[116] amelyet a tagállamok megtilthatnak, kivéve, ha

- ehhez az érintett kifejezett hozzájárulását adta,[117]
- ez az adatkezelő kötelezettségei és meghatározott jogai gyakorlása érdekében szükséges a foglalkoztatási jogszabályok területén,
- ez az érintett vagy más személy létfontosságú érdekeinek védelméhez szükséges abban az esetben, ha az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni,
- ez valamely nonprofit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik, azzal 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,
- ez olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott, vagy amelyek jogi követelések megállapításához, gyakorlásához vagy védelméhez szükségesek, illetve ha
- a kezelés egészségügyi célból történik.[118]

Csak hatóság közreműködésével történhet bűncselekményekre, büntetőítéletekre vagy biztonsági intézkedésekre vonatkozó adatok feldolgozása.[119] Az érintetteket az adatkezelés tényéről, céljáról, valamint az adatfeldolgozó egyes ismérveiről tájékoztatni kell, biztosítani kell számára továbbá az adatokhoz való hozzáférés és az adathelyesbítés jogát.[120]

Mindezen követelményekből a tagállamokra háruló kötelezettségek korlátozhatók a tagállamok által nemzetbiztonsági, honvédelmi, közbiztonsági és bűnmegelőzési okból, valamint abban az esetben, ha valamely tagállam vagy az Unió gazdasági, pénzügyi érdeke, bizonyos hatósági feladatok ellátása valamint az egyének jogainak és szabadságainak védelme úgy kívánja.[121] Tekintettel arra, hogy a terrorizmus elleni harc mind a nemzetbiztonsági, honvédelmi, közbiztonsági és bűnmegelőzési okokat, mind az egyének szabadságának védelmét kimeríti, a biometrikus adatok kezelése is megtörténhet az említett indokokkal. Az Irányelv tartalmazza az ún. automatizált egyedi döntés kategóriáját, amely bizonyos mérlegelést is igénylő értékelések kizárólag automatizált megvalósításán alapul.

[114] Adatvédelmi Irányelv 6. cikk (1) bek.
[115] Adatvédelmi Irányelv 7. cikk a)-f) pont
[116] Ebben a körbe tartoznak a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkozó adatok. Adatvédelmi Irányelv 8. cikk (1) bek.
[117] Ezt azonban a tagállam joga megtilthatja.
[118] Adatvédelmi Irányelv 8. cikk (2) bek. a)-e) pont
[119] Adatvédelmi Irányelv 8. cikk (2)-(5) bek.
[120] Adatvédelmi Irányelv 10. és 12. cikk
[121] Adatvédelmi Irányelv 13. cikk

Ennek a lehetőségét az Irányelv tiltja.[122] A biometrikus azonosítók alkalmazása azonban ilyen jellegű döntésről nem beszélhetünk, így a teljes automatizáltság is megengedett lehet.

Az adatfeldolgozás megfelelő biztonságának érdekében – a technika vívmányaira és alkalmazásuk költségeire tekintettel – ezeknek az Adatvédelmi Irányelv előírásainak olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás kockázatainak és a védendő adatok jellegének.[123] Mindezeknek intézményi garanciáját jelentik azok a kijelölt tagállami felügyelő hatóságok, amelyek feladata az Adatvédelmi Irányelv rendelkezései érvényesülésének tagállami szinten történő vizsgálata.[124]

2. A biometrikus azonosítók alkalmazása

a) Alapvető szabályok

Az Európai Unió biometrikus azonosítókat bevezető jelenlegi szabályozási rendszere több lépésen keresztül alakult ki. 2003. szeptember 24-én az Európai Unió Bizottsága (Bizottság) javaslatot terjesztett az Európai Unió Tanácsa (Tanács) elé[125] az egységes tartózkodási engedély formátumot szabályozó 1030/2002/EK rendelet és az egységes vízum formátumot szabályozó 1683/95/EK rendelet módosítására vonatkozóan.[126] Ez a javaslat tartalmazta a tagállamoknak azt a törekvését, hogy a vízumon és a tartózkodási engedélyen biometrikus azonosítók szerepeljenek. A biometrikus azonosítók közül – technikai és biztonsági tényezőket figyelembe véve – a javaslat elsődlegesen az arckép, másodlagosan az ujjlenyomat alkalmazását támogatta.[127]

A Tanács 2004. június 8-án hozott 2004/512/EK határozatával megalkotta a Vízuminformációs Rendszert (Visa Information System – a továbbiakban: VIS), amely a „nemzeti hatóságok számára lehetővé teszi a vízumadatok bevitelét és frissítését, valamint az adatok elektronikus úton való megtekintését.”,[128] vagyis – egyszerűen megfogalmazva – lehetőséget nyújt a vízumadatok tagállamok közti cseréjére. A VIS központi rendszerből és ezzel, valamint egymással összekapcsolódó ún. nemzeti „interface-ekből” áll, amely struktúra lehetővé teszi a lehető leggyorsabb és legpontosabb információáramlást. A biometrikus adatok szempontjából releváns elem, hogy már a VIS létrehozatalakor előrevetítették a biometrikus azonosítók rendszerbe való beépítését is.

A Tanács 2004. december 13-án a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK számú rendeletében (Rendelet) szabályozta először részletesen az útlevelek és úti okmányok biometrikus elemeinek kérdéskörét. A Rendeletnek, amely a Bizottság COM (2004) 116 számú javaslata nyomán készült, hármas célja volt: az útlevelek biztonságosabbá tétele a harmonizált biztonsági jellemzőkre vonatkozó standardokról kötelezővé tétele révén, ezzel egyidejűleg megbízható kapcsolat létrehozása az irat és annak

[122] Adatvédelmi Irányelv 15. cikk (1) bek.
[123] Adatvédelmi Irányelv 17. cikk (1) bek.
[124] Adatvédelmi Irányelv 28. cikk (1) bek.
[125] COM (2003) 558
[126] Ennek előzménye – a javaslat szövege szerint – a 2003. június 19-20-án Thesszalonikiben tartott ülésén közölt nyilatkozat, miszerint az EU-nak koherens elveket kell követnie a biometrikus azonosítók tekintetében, amelyből természetesen következik az egységes útlevelek, harmadik államok polgárai számára kiállított egységes dokumentumok és egységes vízum információs rendszer alkalmazása.
[127] Ennek megállapítása során figyelembe vették az ICAO által alkalmazott megoldásokat.
[128] 2004/512/EK határozat 1. cikk

tényleges birtokosa között a biometrikus azonosítók bevezetésével, végül pedig annak megvalósítása, hogy az uniós tagállamok számára megfeleljenek az USA vízummentességi programja követelményeinek. A javaslat eredetileg csupán az arckép mint biometrikus azonosító alkalmazását tette volna kötelezővé és a nemzeti jogalkotásra bízta volna az ujjnyomat felvételét az útlevélbe.[129] A Bizottság javasolta továbbá, hogy a biometrikus azonosítókat elegendő tárkapacitással rendelkező adathordozón helyezzék el, ami kapcsolat nélküli chip vagy más, szükséges kapacitással rendelkező adathordozó is lehet.

A javaslatot megvitatta a vízumokkal foglalkozó munkacsoport, majd a bevándorlással, a határokkal és a menekültüggyel foglalkozó stratégiai bizottság is. Végül továbbításra került az Európai Parlamentnek az a végleges javaslati forma, amelyben kötelező jellegű első biometrikus jellemzőként a digitális arckép szerepel, míg választható második biometrikus jellemzőként az ujjnyomat. A Bel- és Igazságügyi Tanács 2004. október 25-26-i ülésén a javaslat szövegét módosították, ismét kötelezővé téve mindkét biometrikus jellemzőt. 2004. december 2-án az Európai Parlament nem kötelező jogalkotási állásfoglalást fogadott el, amelyben támogatta a digitális arcképet tartalmazó útlevél bevezetését, elutasította viszont az ujjnyomatok kötelező felvételét. A 2004. december 2-i jogalkotási állásfoglalás leszögezte, hogy az útlevél biometrikus jellemzői kizárólag az irat eredetiségének és az útlevél birtokosa személyazonosságának ellenőrzésére használhatók, és olyan „különösen biztonságos, megfelelő tárolókapacitással rendelkező adathordozón" kell tárolni azokat, amely „képes biztosítani a tárolt adatok integritását, eredetiségét és titkos jellegét". Az állásfoglalás azt is rögzíti, hogy a biometrikus adatokhoz csak az ezek olvasására, tárolására, helyesbítésére és törlésére jogosult tagállami hatóságok férhetnek hozzá. Végül a Parlament úgy módosította a rendelettervezet szövegét, hogy kifejezetten kikötötte, „nem kerül létrehozásra az európai uniós útlevelek és úti okmányok központi adatbázisa, amely valamennyi uniós útlevél birtokosának biometrikus és más adatait tartalmazza".[130]

A Tanács végül a Bel- és Igazságügyi Tanács 2004. október 25-26-i ülésén kiadott tervezete alapján fogadta el 2004. december 13-án a 2252/2004/EK Rendeletet, amelyben nem vette figyelembe a Parlament javaslatait és módosításra vonatkozó kéréseit. A Rendeletet a biometrikus azonosítók alkalmazásának „alaprendeleteként" tarthatjuk számon a közösségi jogban. Preambulumában deklarált célja, hogy a biometrikus azonosítók révén „az okmány és annak valódi birtokosa között megbízható kapcsolat jöjjön létre", vagyis kiküszöbölje az okmányok csalárd felhasználását.[131] Adatvédelmi indokkal rögzíti, hogy valamennyi tagállamnak egyetlen szervet kell kijelölnie az útlevelek és más úti okmányok előállítására, utal továbbá arra, hogy az útlevelekkel és úti okmányokkal összefüggésben felmerülő adatkezelésre a 95/46/EK irányelv szabályait kell alkalmazni. Az arányosság követelményének való megfelelés érdekében a rendelet leszögezi, hogy a benne foglalt rendelkezések által alkalmazott jogkorlátozások nem lépik át a Schengeni Megállapodás végrehajtásához szükséges mértéket.

[129] Hornung: i. m. 255. o.

[130] Vö. a 29. cikk szerinti Adatvédelmi Munkacsoport 2/2005-ös véleményét a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról. Hivatalos Lap L 385., 2004.12.29. (a továbbiakban: Az Adatvédelmi Munkacsoport véleménye)

[131] A rendelet kimondja, hogy az itt szereplő „előírásokat olyan előírásokkal kell kiegészíteni, amelyek a hamisítás és a meghamisítás veszélyének megelőzése érdekében titkosak lehetnek". Preambulum (5) pont

A rendelet az ICAO által általánosan elfogadott biometrikus azonosítók alkalmazását írja elő: az arcképet tartalmazó tárolóelemet, továbbá ún. interoperábilis formátumban belefoglalt ujjnyomatokat.[132] Azok a személyek, akik számára útlevelet vagy úti okmányt állítottak ki, jogosultak arra, hogy ellenőrizzék az útlevélben vagy az úti okmányban tárolt személyes adatokat, és szükség esetén azok helyesbítését vagy törlését kérjék.[133] További adatvédelmi intézkedést jelent, hogy az útlevél vagy úti okmány kizárólag olyan géppel olvasható információt tartalmazhat, amelyet e rendelet vagy annak melléklete megállapít, illetve amelyet a kiállító tagállam nemzeti jogszabályainak megfelelően az útlevélben vagy az úti okmányban említ. Végül a biometrikus adatok tekintetében – megelőzve a visszaéléseket – a biometrikus jellemzők kizárólag az okmány valódiságának, valamint az okmánybirtokos személyazonosságának ellenőrzésére használhatók fel.[134] Ez az előírás tehát tiltja a biometrikus azonosítókból eredő további következtetések levonását, vagyis további személyes adatok kinyerését.

Az alaprendelet elfogadása után számos további szabályozási javaslat és jogszabály született a biometrikus azonosítókra vonatkozóan. 2004. december 28-án nyújtotta be a Bizottság javaslatát a VIS-re, és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjére vonatkozó rendelet kiadására,[135] amelyet 2008-ban fogadtak el, hatályba lépése folyamatban van.[136] A műszaki biztonságot elősegítendő, 2005. február 28-án a Bizottság határozatot hozott[137] a tagállamok által kiállított útlevelekben és úti okmányokban alkalmazott biztonsági jellemzők és biometrika szabványaira vonatkozó műszaki előírásokról. E dokumentum a beépített chip-pel rendelkező útlevelekre vonatkozóan tartalmaz szabályozást, alapul véve az ICAO ajánlásait. Részletesen meghatározza továbbá az adathordozóval szemben támasztott követelményeket, és rögzít bizonyos adatvédelmi és adatbiztonsági elveket is. 2006. június 28-án a Bizottság újabb határozatával[138] egészítette ki a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírások műszaki követelményeit. 2006. szeptember 22-én a Bizottság szintén határozatban szabályozta a Vízuminformációs Rendszer kifejlesztésével kapcsolatos biometrikus jellemzőkre vonatkozó szabványokról szóló műszaki előírások megállapításáról.

b) A szabályozás értékelése

A 2252/2004/EK Rendelet megszületése után, de részben még az azt követő műszaki szabványok és módszerek megállapítása előtt több uniós és egyéb szervezet is kifejtette álláspontját a biometrikus azonosítók alkalmazásával összefüggésben. 2005. szeptember 16-án Montreux-ben ült össze az adatvédelmi és a magánélet védelmével

[132] 2252/2004/EK 1. cikk (2) bek. A rendelet 6. cikke értelmében a tagállamoknak állampolgáraik útlevelébe a digitális arcképet 2006. augusztus 28-ig kell bevezetniük, az ujjnyomatokat pedig 2008. február 28-ig.
[133] Mindez természetesen csak úgy érvényesülhet, hogy nem sérülnek az adatvédelmi szabályok. 2252/2004/EK 4. cikk (1) bek.
[134] 2252/2004/EK 4. cikk (2)-(3) bek.
[135] COM(2004) 835
[136] Vö. http://www.europarl.europa.eu/oeil/file.jsp?id=5223192 &noticeType=null&language=en (2008. 07. 25.)
[137] COM(2005) 409
[138] C(2006) 2909

foglalkozó biztosok 27. nemzetközi konferenciája, amely állásfoglalást[139] fogadott el a biometrikus adatok útlevelekben, személyazonosító igazolványokban és úti okmányokban való alkalmazásáról. Az állásfoglalás egyrészt rögzíti azt a felismerést, hogy manapság már nem csupán a közhatalmat gyakorló szervek, hanem a magánszférában tevékenykedő személyek, szervezetek is gyakran alkalmaznak biometrikus azonosítókat – legtöbbször persze beleegyezéses alapon –, amelyet azonban a biometrikus azonosítók felhasználásáról rendelkező jogszabályok nem szabályoznak. Másrészt figyelembe veszi, hogy a biometrikus adatok gyűjtése az érintett tudta nélkül is könnyen végbemehet, hiszen az egyének öntudatlanul is hagyhatnak maguk után biometrikus nyomokat. Végül leszögezi, hogy a biometrikus azonosítók alkalmazása az emberi testet magát teszi „géppel olvashatóvá", így az egyén általános azonosítása is lehetővé válik. Mindezeknek megfelelően a biztosok konferenciája kívánatosnak tartotta a) a hatékony védelmet a biometrikus azonosítók jellegéből adódó, inherens kockázatokkal szemben, b) a jogszabályi kötelezettségen alapuló, közcélokra végzett, valamint a beleegyezésen alapuló, szerződéses (magán)célokra végzett adatgyűjtés és -tárolás határozott elkülönítését, végül c) a biometrikus azonosítók alkalmazásának technikai korlátozását kizárólag azonosítási célokra.

A 95/46/EK Adatvédelmi Irányelv 29. cikke alapján felállított személyesadat-feldolgozás vonatkozásában az egyének védelmével foglalkozó munkacsoport[140] (Munkacsoport) véleménye a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról szintén több problémát és veszélyt fogalmaz meg a biometrikus azonosítók alkalmazásával kapcsolatban.[141] Ezek a fenntartások alapvetően két kérdéskör köré csoportosíthatók: a) a tároló adatbázisok és az azonosítási folyamat biztonságos voltának problémája, b) a biometrikus azonosítók testi jellemzőkkel való sajátos kapcsolata és az ebből levonható következtetések nyomán kialakuló visszaélések lehetősége.

Az első kérdéskörrel kapcsolatosan kritika tárgya, hogy a korábban a biometrikus jellemzőknek csupán leírását tartalmazó dokumentumokkal szemben az új dokumentumok e jellemzőket digitalizált formában tartalmazzák, amely lehetővé teszi a jellemzők adatbázisokban való tárolását és könnyű elérhetőségét, előre egzakt módon nem jelezhető célokra. A biometrikus azonosítókat tároló adatbázisokkal kapcsolatban gondot jelenthet, hogy azonban az egyes államok szinte felbecsülhetetlen mennyiségű szenzitív információt lesznek képesek felhalmozni, így rendkívül jelentős információmennyiség van kitéve a jogosulatlan hozzáférésnek. Az egész Európai Unióra kiterjedő központi adatbázis pedig még inkább növelné e visszaélések veszélyét. További technikai kockázat az azonosítás folyamata az ún. RFID-chip[142] alkalmazásával, amely rádiókapcsolat segítségével végzi el az adatok leolvasását. Mivel az RFID-chip és a leolvasó közötti kapcsolat „lehallgatható",

[139] 27th International Conference of Data Protection and Privacy Commissioners Montreux 16 September 2005. Resolution on the use of biometrics in passports, identity cards and travel documents. http://www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf (2007. 12. 10.)

[140] A munkacsoport tanácsadói státuszban működik és függetlenül jár el, a tagállamok által kijelölt felügyelő hatóság(ok) képviselőjéből, a közösségi intézmények és szervek nevében létrehozott hatóság(ok) képviselőjéből, továbbá a Bizottság egy képviselőjéből áll. A tagokat azok az intézmények vagy hatóságok jelölik ki, amelyeket a tagok képviselnek. Vö. az Adatvédelmi irányelv 28. cikk (1)-(2) bekezdésével.

[141] Vélemény a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet végrehajtásáról. Hivatalos Lap L 385., 2004.12.29., 1–6. o.

[142] Rádiófrekvenciás azonosító chip.

az információ jogosulatlanok számára is hozzáférhetővé válhat. Ezt hivatott megakadályozni az ún. „Basic Access Control”[143] (BAC) módszer alkalmazása. Ez biztosítja, hogy az adatokhoz való hozzáférés csak akkor legyen lehetséges, ha az adatok chipről való leolvasása előtt az útlevél és a leolvasó közötti kapcsolat révén az útlevél géppel olvasható zónájából egyfajta hozzáférési kulcs, ún. „Document Basic Access Key” kerül felépítésre. Ez a hozzáférési kulcs az útlevélszámból, a születési időpontból és a lejárati dátumból számítódik. A leolvasó csak a hozzáférési kulcs felépítése után képes olvasni az RFID-chipen tárolt adatokat. A BAC rendszer azonban nem jelent elégséges biztonsági intézkedést. Az útlevél géppel olvasható sávján tárolt adatok ugyanis nem mindig titkosak, számos államban az irat birtokosának fel kell fednie ezeket a hatóságok előtt. A BAC felépítéséhez szükséges információ tehát nem minden esetben marad rejtve. Megoldást jelenthet a kiterjesztett hozzáférési kulcs „Extended Access Key” alkalmazása, amely bonyolultabb, ezért biztonságosabb rendszer is. Ez a technológia azonban nem biztosított valamennyi tagállamban.

A második kérdéscsoportba tartozik az a probléma, hogy a biometrikus azonosítók köre testi jellemzőket takar, amely egyrészt következtetéseket tehet lehetővé további testi jellemzőkre vagy állapotra (elsősorban az egészségi állapotra) vonatkozóan,[144] másrészt kizárhat meghatározott testi fogyatékossággal rendelkezőket az azonosítási folyamatból, illetve ezeket a személyeket szükségtelen kellemetlenségeknek teheti ki. Járulékos, lélektani hatással összefüggő kérdés az, hogy a biometrikus adatokat korábban általában bűnüldözési célokra használták, ami nehezítheti az új azonosítási módszerek társadalmi elfogadottságát.

c) A legújabb módosítási javaslatok és ezek értékelése

2007. október 18-án a Bizottság a 2252/2004-es Rendelet módosítását javasolta,[145] mivel nyilvánvalóvá vált – talán a Munkacsoport véleményének hatására is –, hogy bizonyos esetekben az egyén nem képes biometrikus adatot szolgáltatni, illetve biometrikus azonosításnak alávetni magát, vagy biometrikus adatai nem elég megbízhatóak. A Javaslathoz fűzött magyarázat szerint a módosítás célja az, hogy kiküszöbölje a Rendelet hiányosságait, az eredeti szöveg ugyanis nem jelöl meg kivételeket az ujjnyomatvétel alól. A módosítás két csoport vonatkozásában tenne kivételt az ujjnyomatvétel alól: 6 év alatti gyermekek és olyan testi fogyatékossággal rendelkezők esetében, akik nem képesek ujjnyomatot adni. A módosítás magyarázata a következő volt: „*Néhány tagállam kísérleti projektje során azt tapasztalták, hogy a hat év alatti gyermekek ujjnyomata nem megfelelő minőségű ahhoz, hogy egyértelműen igazolja a személyazonosságot. Ezen túlmenően az ujjnyomatok ebben a korban még jelentős változáson mennek keresztül, ami megnehezíti azok ellenőrzését az útlevél érvényességének teljes időtartama alatt. Sem jogi, sem biztonsági szempontból nem lenne célszerű, ha nemzeti jogszabályok határoznák meg, hogy ki mentesül a tagállamok által kiállított útlevelek és úti okmányok céljából történő ujjlenyomat-adási kötelezettség alól. Következésképpen a Bizottság javasolja a 2252/2004/EK rendelet módosítását annak érdekében, hogy egységes kivételek*

[143] Alapvető hozzáférési ellenőrzés.

[144] Az ujjnyomatok tárolása kapcsán például meghatározható bizonyos redőzeti minták és meghatározott betegségek közötti kapcsolat. Egyes papilláris minták például statisztikai korrelációt mutatnak a rákbetegség bizonyos típusaival. Ezekkel a korrelációkkal kapcsolatban egyelőre tudományos vita folyik, amelyet azonban nem lehet figyelmen kívül hagyni.

[145] COM(2007) 619 végleges (Javaslat)

érvényesüljenek: a hat év alatti gyermekeket, valamint azon személyeket, akik fizikailag nem képesek ujjlenyomatot adni, fel kellene menteni e kötelezettség alól."[146] Ezen túlmenően kiegészítő biztonsági intézkedésként és a gyermekek további védelme érdekében bevezetésre kerülne az „egy személy-egy útlevél" elv.[147] A kapcsolódó magyarázata szerint ez az elv biztosítaná, hogy az útlevél és a biometrikus adatok csak az útlevél tulajdonosának személyéhez legyenek köthetők. Amennyiben a kiállított útlevél a személy gyermekeire is érvényes lenne, de csak nevüket tüntetné fel, fényképüket nem, akkor a gyermekek személyazonosságát nem lehetne megbízható módon ellenőrizni, és ez növelhetné a gyermekkereskedelem kockázatát.

A Javaslatot az Európai Adatvédelmi Biztos (Biztos) értékelte; véleményét 2008. április 19-én hozta nyilvánosságra.[148] A Biztos által megfogalmazott kritikák kétirányúak voltak: a) egyrészt érintették a Javaslat-tervezet eljárási kérdéseit, b) másrészt észrevételeket fogalmaztak meg a jövendő szabályozással kapcsolatban. Az eljárási elégtelenségekkel összefüggésben a Biztos nehezményezte, hogy a Bizottság nem tett eleget annak a kötelezettségének, hogy – a 45/2001/EK rendelet[149] 28. cikk (2) bekezdésében[150] foglalt előírás szerint – konzultáljon a Biztossal e személyes adatok védelmét érintő kérdésben. Másrészt a Bizottság nem végzett előzetes hatásvizsgálatot sem, amely megkérdőjelezi a Javaslat szükségességére és arányosságára vonatkozó értékelést.

A Javaslat érdemét tekintve a Biztos üdvözölte a Bizottság arra vonatkozó törekvéseit, hogy kivételeket építsen be a 22525/2004/EK rendelet szabályai közé, ezek a kivételek azonban a Biztos szerint még mindig elégtelenek mivel nem említenek minden olyan esetet, ahol a biometrikus rendszerek tökéletlensége, azonosításra nem alkalmas volta felmerül, ami különösen a gyermekek és az idősek szempontjából releváns.[151] A Biztos megkérdőjelezte a kísérleti projekteket eredményességét, mivel ezek nem nyújtottak elégséges információt a Bizottság módosító Javaslatához. A Javaslatban meghatározott életkori határt mindezek fényében indokolt ideiglenesnek tekinteni, ezért három év elteltével felül kell vizsgálni, és részletes tanulmányokkal, valamint kísérletekkel kell alátámasztani. Az alsó korhatár mellett a Biztos felső korhatár megállapítását is javasolta, mivel egyes kutatások kimutatták, hogy az ujjnyomatok azonosításának megbízhatósága az idősek esetében is csökken. Erre vonatkozóan is kívánatosnak tartotta további kutatások elvégzését. A Biztos ráirányította a figyelmet továbbá arra, hogy nincs pontosan meghatározva, milyen minőségű biometrikus mintát, ujjnyomatokat fogadnak, illetve utasítanak el az azonosítást végző rendszerek, vagyis mekkora az azonosítás elfogadott „hibaszázaléka". Ezért javasolta olyan határ megvonását, amely valamennyi államban azonos, mivel ennek hiányában az azonosítási folyamat függ attól, hogy az egyén a

[146] COM(2007) 619 final 120. pont
[147] Ennek az elvnek az alkalmazását az ICAO is ajánlja.
[148] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. 26. 03. 2008. Hozzáférhető: http://www.pdfdownload.org/pdf2html/pdf2html.php?url=http%3A%2F%2Fedps.europa.eu%2FEDPSWEB%2Fwebdav%2Fsite%2FmySite%2Fshared%2FDocuments%2FConsultation%2FOpinions%2F2008%2F08-03-26_Biometrics_passports_EN.pdf&images=yes (2008. 04. 19.)
[149] A személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról.
[150] „Ha a Bizottság a személyek jogainak és szabadságainak a személyes adatok feldolgozásával kapcsolatos védelmére vonatkozó jogalkotási javaslatot fogad el, az európai adatvédelmi biztossal egyeztet."
[151] Opinion of the European Data Protection Supervisor 10. pont

schengeni határ mely részén kíván átlépni. Mindezek elvezetnek a közös azonosítási standardok bevezetéséhez.

C) A személyes és a biometrikus adatok védelmének alkotmányjogi szabályozása Magyarországon

Az Alkotmány 59. §-a rögzíti, hogy a Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog. Az Országgyűlés – az alkotmányi felhatalmazás alapján – a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) megalkotásával végezte el az adatvédelem részletes szabályozását.[152] Az Avtv. megalkotásának közvetlen előzménye a 15/1991. (IV. 13.) AB határozat volt, amelyben az Alkotmánybíróság megállapította, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám), valamint a személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes.[153]

A személyes adatok védelméhez való jogot az Alkotmánybíróság nem hagyományos védelmi jogként, hanem annak aktív oldalát is figyelembe véve, tágabb értelemben, információs önrendelkezési jogként értelmezi és alkalmazza. E jog tartalma, hogy mindenki maga rendelkezik magántitkainak és 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 az Alkotmány 8. §-ában megkövetelt feltételeknek.”[154]

Az információs önrendelkezési jog alkalmas arra, hogy az érintett összes, adatkezeléssel kapcsolatos személyiségi jogának foglalatát adja. Az információs önrendelkezés legfontosabb garanciái az adatkezelés célhoz kötöttségének elve, továbbá az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása.[155] Az alkotmányi és a törvényi szabályozás azonban az információs önrendelkezést nem, csupán a személyes adatok védelmét garantálja, amelynek a korlátozás szempontjából vannak következményei.

---

[152] Legutóbbi módosítás: 2005. évi XIX. törvény

[153] Az indítványozó teljes egészében támadta az állami népességnyilvántartásról szóló 1986. évi 10. törvényerejű rendeletet és két végrehajtási rendeletét, azzal, hogy ezek a személyi adatok védelméhez való alkotmányos joggal (Alkotmány 59. §) ellentétesek. Az AB a szabályozást megsemmisítette, és az Országgyűlést törvényalkotásra hívta fel: „*A törvényhozó kötelessége, hogy megalkossa az Alkotmány 59. és 61. §-ának megfelelő törvényt a személyes adatok védelméről és a közérdekű információk hozzáférhetőségéről, továbbá, hogy az abba lefektetett alapelveket ún. területspecifikus törvényekben konkretizálja. A törvényhozó felelőssége eldönteni, hogy az Alkotmánybíróság által megsemmisített személyi számot immár korlátok között ismét bevezeti-e, s hogy ez esetben milyen megszorításokat alkalmaz és milyen speciális ellenőrzést épít ki*.”

[154] 15/1991. (IV. 13.) AB határozat

[155] Petrétei József: Az információs önrendelkezés és az információs szabadság. Kézirat, Pécs 2002.

1. A személyes adatok köre

A személyes adat meghatározott természetes személlyel – az érintettel – kapcsolatba hozható adat, és az adatból levonható, az érintettre vonatkozó következtetés.[156] A személyes adatok körébe mindaz beletartozik, ami az élő személlyel[157] kapcsolatos bárminemű információt hordoz, függetlenül attól, hogy arra az érintett mennyire érzékeny.[158] Személyes adat tehát az érintettre vonatkozó vélemény, minősítés, továbbá az adatokból levonható következtetés is, amely az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.[159] Látható, hogy ebbe a tág fogalom-meghatározásba bármiféle biometrikus adat beletartozhat.[160] Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete[161] elrendeli.[162]

Az Avtv. meghatározza és megkülönbözteti egymástól az adatkezelés és adatfeldolgozás, valamint az adatkezelő és adatfeldolgozó fogalmát. Az 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.[163] Az Avtv. e fogalom-meghatározás keretében példálózó jelleggel említ néhány biometrikus adatot, de azokkal kapcsolatban nem határoz meg különös adatkezelési szabályokat. A gyakorlatban a biometrikus adatok felvétele és sablonná alakítása kritikus szakaszt jelent, amelynek során az adatvédelmi garanciáknak fokozottan kell érvényesülnie. A korábban említetteknek megfelelően, egyes biometrikus azonosítók (pl. ujjnyomat, DNS-minta, térfigyelő rendszerben rögzített képmás) gyűjtése megtörténhet az érintett tudta nélkül is: az ilyen esetekre *speciális garanciák szükségesek* az adatvédelmi szabályok érvényesítéséhez.[164]

---

[156] Avtv. 2. § 1. pont

[157] Az információs önrendelkezési jog szükségképpen az adattal érintett *élő* személyt illeti meg. A meghalt személy adatainak védelméről, illetőleg a velük való rendelkezésről – az adattal vagy az adatkezeléssel összefüggő – külön jogszabályok (pl. a Ptk., a levéltári, az anyakönyvi jogszabályok) szólnak. Lásd a 3.§-hoz fűzött indokolást.

[158] Mivel ez kizárólag tőle, egyéniségétől, körülményeitől, társadalmi helyzetétől, az adott tényállástól stb. függ. Lásd a 2.§-hoz fűzött indokolást.

[159] 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.

[160] Szabó Máté Dániel: Biometrikus azonosítás és adatvédelem. Acta Humana 15. évfolyam 2004. 1. szám 85. o.

[161] A helyi önkormányzatok feladatkörének bővülése, önállóságuk növekedése azzal jár, hogy feladatuk ellátása szükségessé teheti a területükön a lakosság vagy az ott működő szervezetek olyan adatainak a kezelését, amelyekről központi jogszabály nem rendelkezik. Ezért a helyi önkormányzat számára is lehetővé kell tenni, hogy – törvényben meghatározott körben – rendeletében az adatkezelést előírhassa. Lásd az Avtv. indokolását.

[162] Avtv. 3. § (1) bek.

[163] Avtv. 2. § 9. pont

[164] Szabó: i. m. 84. o.

2. A különleges adatokra vonatkozó szabályok

Az Avtv. szerint különleges (szenzitív) adat a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra,[165] a vallásos vagy más meggyőződésre, az érdekképviseleti szervezeti tagságra, továbbá az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi[166] személyes adat.[167] A szenzitív adatok körének törvényi rögzítése problematikus lehet a biometrikus azonosítók egységes kezelése esetén, mivel bizonyos esetekben bizonyos típusú biometrikus azonosítók a különleges adatok kategóriájába tartozhatnak, illetve azok bizonyos kombinációja az egészségi állapotról adhat információt, illetőleg bűnügyi személyes adatként jelentkezhet.

A különleges adatok (szenzitív, érzékeny) adatok fokozottabb védelemben részesülnek, mivel az egyenlő méltóság csak úgy biztosítható, ha a hátrányos vagy kivételes megkülönböztetésre lehetőséget nyújtó adatok kiszolgáltatásában a lehető legnagyobb mértékben érvényesül az egyén információs önrendelkezésének joga. Különleges adat ezért csak akkor kezelhető, ha

- az adatkezeléshez az érintett írásban hozzájárul,
- vagy a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, érdekképviseleti szervezeti tagságra, illetve a vallásos, illetőleg más meggyőződésre vonatkozó adatok esetében ez nemzetközi egyezményen alapul, vagy Alkotmányban biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény rendeli el,
- egyéb esetekben, ha a különleges adat kezelését törvény elrendeli.[168]

3. A biometrikus azonosítókra vonatkozó szabályozás

Az európai uniós csatlakozással Magyarország számára is kötelezővé vált a közösségi jog végrehajtása, illetve implementálása a belső jog rendszerébe. Az Unió Adatvédelmi Irányelvének beillesztése a magyar jogban több jogszabály módosításával valósult meg, amelyek közül kiemelhető az alapvető adatvédelmi jogszabálynak tekintendő Avtv. A tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet előírásainak végrehajtása érdekében szükségessé vált a magyar szabályozás módosítása is. A külföldre utazásról szóló 1998. évi XII. törvény (Utv.) módosításával sor került az ideiglenes magánútlevél adattartalmának a magánútlevél adattartalmához történő

[165] Az Alkotmánybíróság azonban megállapította, hogy „*...a jogállamban közhatalmat gyakorló vagy a politikai közéletben résztvevő személyek – köztük azok, akik a politikai közvéleményt feladatszerűen alakítják – arra vonatkozó adatai, hogy korábban a jogállamisággal ellentétes tevékenységet folytattak, vagy olyan szerv tagjai voltak, amely korábban a jogállamisággal ellentétes tevékenységet folytatott, az Alkotmány 61. § szerinti közérdekű adatok.*" 60/1994. (XII. 24.) AB határozat

[166] 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.

[167] Avtv. 2. § 2. a)-b) pont

[168] Avtv. 3. § (2) bek.

hozzáigazítására, valamint a biometrikus elemeknek az útlevelekbe történő beépítéséhez szükséges jogi háttér megteremtésére. A módosítást követően – amelyet a 2006. évi XXI. törvénnyel végzett el a jogalkotó – az Utv. rögzíti, hogy az útlevél – kivéve a tizenkét hónapra vagy annál rövidebb érvényességi időre szóló ideiglenes magánútlevél – biometrikus azonosítót tartalmazó tároló elemet (tároló elem) tartalmaz.[169] Az adatoknak a tároló elemben történő tárolását olyan technikai módszerek alkalmazásával kell megvalósítani, amelyek a technikailag elérhető legmagasabb szinten biztosítják azt, hogy a tároló elem tartalmához illetéktelen személyek ne férhessenek hozzá.[170] Az útlevélhatóság kizárólag az úti okmány előállításának időtartamára kezelheti az adatokat, és azokat az úti okmány kiadásakor haladéktalanul törölnie kell,[171] a határforgalom-ellenőrzést végző szerv pedig kizárólag a személyes adatnak a tároló elemből történő olvasásával kezelheti a tároló elem által tartalmazott személyes adatokat.[172]

Többek között a Rendelet végrehajtásához tartozó jogalkotási eredmény az is, hogy a Magyar Köztársaság a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról szóló 2007. évi I. és a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló 2007. évi II. törvény hatálybalépése – 2007. július 1-je – óta eltérő szabályozást alkalmaz az EU állampolgárok és a nem EU állampolgárok országhatárok átlépésével kapcsolatban. Az előbbi törvény 60. §-a értelmében a beutazási és tartózkodási tilalom betartásának ellenőrzése céljából az idegenrendészeti kiutasítást elrendelő vagy a bírósági kiutasítást végrehajtó hatóság rögzíti annak a személynek az arcképmását, valamint ujjnyomatát, akit a bíróság kiutasított, vagy akivel szemben az eljáró hatóság a kiutasítással együtt beutazási és tartózkodási tilalmat rendelt el. Az érintett személy az arcképmása, valamint ujjnyomata rögzítését tűrni köteles. Ugyanezen törvény 78. § (1) f) pontja alapján az eljárást végző hatóság nyilvántartásba veszi az arcképmást és az ujjnyomatot, és azt a beutazási és tartózkodási tilalom időtartama alatt kezeli.[173] A 2007. évi II. törvény értelmében többszöri eljárás megakadályozása, valamint a személyazonosság megállapítása céljából a Magyar Köztársaság területének elhagyására kötelező, az idegenrendészeti kiutasítást, a kijelölt helyen való tartózkodást, a beutazási és tartózkodási tilalmat, valamint idegenrendészeti őrizetet elrendelő, illetve a bírósági kiutasítást végrehajtó hatóság rögzíti a harmadik országbeli állampolgár arcképmását, valamint ujjnyomatát. Az érintett az arcképmása, valamint az ujjnyomata rögzítését tűrni köteles.[174] A törvény alapján az idegenrendészeti hatóság a kiadott vízum, illetve más hasonló engedély[175] alapján[176] kezelheti az érintett személy arcképmását az eljárás befejezésétől számított öt évig. Az idegenrendészeti hatóság kezelheti a Magyar Köztársaság területének elhagyására kötelezett, a kijelölt helyen tartózkodásra kötelezett, az idegenrendészeti

[169] Utv. 7. § (2) bek.
[170] Utv. 32/A. § (2) bek.
[171] Utv. 32/A § (1) a) pont
[172] Utv. 32/A § (1) b) pont
[173] 2007. évi I. törvény 78. § (4) bekezdés
[174] 2007. évi II. törvény 53. §
[175] Vízumot helyettesítő engedély, a tartózkodási engedély iránti kérelem a kiadott tartózkodási engedély, az ideiglenes tartózkodásra jogosító igazolás, a kiadott bevándorlási engedély és letelepedési engedély, az ideiglenes letelepedési engedély, nemzeti letelepedési engedély vagy EK letelepedési engedély iránti kérelem és kiadott ideiglenes letelepedési engedély, nemzeti letelepedési engedély vagy EK letelepedési engedély.
[176] Lásd erről bővebben a 2007. évi II. törvény 95, 96, 98, 99. § -ait.

kiutasítás, bírói kiutasítás, a beutazási és tartózkodási tilalom, valamint idegenrendészeti őrizet hatálya alatt álló harmadik országbeli állampolgár az arcképmását és ujjnyomatát[177]

D) A biometrikus adatok mint személyi azonosítók alkalmazásának értékelése

A biometrikus azonosítók alkalmazása progresszív új technikának tűnik a személyek azonosítása területén. Lehetővé teszi, hogy a személyazonosság megállapítása, illetve igazolása gyorsabbá és biztonságosabbá váljon, valamint csökkenti a csalások lehetőségét. Előrevetíthető, hogy a biometrikus adatok – amelyek valószínűleg központosított és interoperábilis rendszerekben kerülnek majd tárolásra – nem csupán részét képezik majd egyes személyi okmányoknak, hanem helyettesíthetik magát a teljes dokumentumot. Nem hagyható azonban figyelmen kívül, hogy ez a jövőkép, sőt, a jelenlegi helyzet is számos etikai és jogi kérdést vet fel az adatédelem területén.

I. A biometrikus azonosítók alkalmazása és a személyi integritás megőrzése

1. Az egyén instrumentalizálásának kérdése

Az emberi testnek, illetve részeinek instrumentalizálása az élethez és emberi méltósághoz való jog fényében tiltottnak minősül, hiszen a jól ismert etikai elv nyomán az ember mindig csak cél lehet, soha nem szolgálhat eszközként valamely cél elérésére.[178] A biometrikus azonosítók alkalmazása, illetve az erre a célra szolgáló adatgyűjtés felfogható úgy is, mint az emberi test egyes vonásainak eszközként való "felhasználása". Az egyén természetes fizikai megjelenése e – az egyén egyediségének tárgyiasítását jelentő – felfogás szerint pusztán meghatározott mennyiségű, megbízhatóan azonosítható adatok halmaza, nem pedig a "legmagasabb rendű élőlény"[179] jellegzetessége. Ezt hivatott megakadályozni az emberi méltósághoz való jog, amelyet szokás az ún. „általános személyiségi jog" egyik megfogalmazásának tekinteni. Az Alkotmány és az alkotmánybírósági értelmezés az átalános személyiségi jog különféle aspektusait nevesíti: a személyiség szabad kibontakoztatásához való jogot, az önrendelkezés szabadságához való jogot, általános cselekvési szabadságot, a magánszférához való jogot. Az általános személyiségi jog védendő értékei közé különösen az egyén magánszférája, a bizalmas szférája, az intim szférája, a becsülete és az információs önrendelkezése sorolható. Az Alkotmány e tényezők védelme révén biztosítja az egyénnek a személyes integritáshoz való jogát. Ezáltal tekintettel van arra a pszichológiai tényre, hogy az egyén önbecsülése és identitása előfeltételezi a magánélet – a közhatalom és harmadik személy általi – támadhatatlan szférájának lehetőségét.[180]

Amennyiben figyelembe vesszük, hogy a fizikai vonások az egyén legintimebb szférájához tartoznak, e vonások, adatok kezelése és az állami beavatkozás ebben a szférába, veszélyeztetheti az egyén általános integritását.

---

[177] 2007. évi II. törvény 102. § (1) b) pont.

[178] „*[A]z ember és általában minden eszes lény öncélként létezik, s nem pusztán eszközként, amely egy másik akarat tetszés szerinti használatára szolgál; mindegyiket, akár magára, akár más eszes lényekre irányuló cselekedetében mindenkor egyúttal célnak is kell tekinteni.*" Immanuel Kant: Az erkölcsök metafizikájának alapvetése. Gondolat Kiadó, Budapest 1991. 60. o.

[179] Chronowski N. – Drinóczi T. – Petrétei J. – Tilk P. – Zeller J.: Magyar Alkotmányjog III. Alapjogok. Dialóg Campus Kiadó, Budapest-Pécs 2006. 54. o.

[180] Chronowski – Drinóczi – Petrétei – Tilk – Zeller: i. m. 60. o.

2. Szükségesség és arányosság

Természetesen a személyes integritás – mint ahogy más alapjogok – nem fogható fel abszolút jogként. Az egyén személyes integritása annyiban korlátozódik, amennyiben az egyén kapcsolatba lép más egyénekkel, a társadalom többi tagjával.[181] Mások céljai és érdekei alapját képezhetik a személyes integritás korlátozásának. E tények elfogadása esetén is felmerül azonban a kérdés, hogy mindenképpen csak a biometrikus azonosítók alkalmazása nyújthat véglegesen megfelelő biztonságot a személyazonosítás területén.

Az Alkotmánybíróság az alapjogok tartalmának feltárása, és a korlátozás terjedelme szempontjából fontos doktrínákkal gazdagította a magyar alkotmányjogot,[182] amikor az alapjogok korlátozásával összefüggésben kialakította az ún. alapjog-korlátozási teszteket.[183] Az általános alapjog-korlátozási teszt az ún. szükségességi-arányossági teszt, amely szerint az állam akkor élhet az alapjog-korlátozás eszközével, ha más alapjog védelme vagy érvényesülése, illetve egyéb alkotmányos cél védelme másként nem érhető el. E feltétel fennállása esetén is irányadó, hogy az állam csak a feltétlenül szükséges mértékben korlátozhat. Mindezeknek megfelelően alkotmányos a korlátozás, ha

- az nem az alapjog érinthetetlen lényegére vonatkozik,
- elkerülhetetlen, kényszerítő okkal történik (vagyis más alapjog, alkotmányos cél, vagy elvont alkotmányi érték[184] védelme semmilyen más módon nem érhető el),
- mértéke a cél fontosságával arányos, és az okozott sérelmek enyhítésére garanciák állnak rendelkezésre.

A személyes adatok védelméhez való jog korlátozásával, vagyis ebben a kontextusban a biometrikus adatok kezelésével összefüggésben a meghatározott cél, amelyet nemzetközi és szupranacionális szerződések, dokumentumok, valamint közvetetten az Alkotmány is említ, a terrorizmus elleni harc. Kérdés, hogy e cél fényében a biometrikus azonosítók felhasználása összhangban van-e a szükségesség követelményével, hiszen az az álláspont is alátámasztható, miszerint a terrorizmus leküzdése más eszközökkel (pl. hagyományos aznosítók alkalmazásával) is elérhető. Az arányosság elve nem pusztán a korlátozás mértékére, hanem annak formai követelményeire is vonatkozik. Ebből következően a biometrikus adatok kezelése kizárólag törvény általi felhatalmazáson alapulhat. A magyar szabályozás ezen a téren egyelőre nagyrészt elégtelen.

II. A magyar szabályozással kapcsolatban felvetődő problémák

Amint az a korábbiakban említésre került, az Avtv. úgy határozza meg a személyes adatok fogalmát mint bármely, a természetes személlyel kapcsolatba hozható adatot, és az ebből levonható következtetést. A különleges (szenzitív) adat pedig az Avtv. szerint a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre, az érdekképviseleti szervezeti tagságra,

[181] Chronowski – Drinóczi – Petrétei – Tilk – Zeller: i. m. 60. o.
[182] Vö. Sári János: Alapjogok. Alkotmánytan II. Osiris Kiadó, Budapest 2001.
[183] Holló – Balogh (szerk.): Az értelmezett alkotmány. Magyar Hivatalos Közlönykiadó, Budapest 2005. 143. o.
[184] Más cél vagy elvont alkotmányi érték például: nyomós közérdek, köznyugalom, jogbiztonság, hatalommegosztás. 58/1994. (XI. 10.) AB határozat, ABH 1994. 334, 338, 30/1992. (V. 26.) AB határozat, ABH 1992. 167, 171. Vö. Chronowski – Drinóczi – Petrétei – Tilk – Zeller: i. m. 29. o.

továbbá az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat. E meghatározások egyike sem nevesíti kifejezetten a biometrikus adatok körét, amelyből következően nehéz integrálni ezen adatok fogalmát az Avtv. rendszerébe. A különleges adatok közül egyes elemek – elsősorban a testi jellegzetességekre és egészségi állapotra vonatkozók – ugyan kapcsolatba hozhatók a biometrikus adatokkal, de a biometrikus adatok köre mint sajátos adatcsoport nem tartozik a különleges adatok közé.

A törvényi meghatározásokat figyelembe véve egyértelmű, hogy a biometrikus adatok személyes adatok, de sajátos vonásaik miatt indokolt lenne, hogy – legalább egyes biometrikus adatok – a különleges adatok körébe tartozzanak, vagy különös szabályozást kapjanak az adatgyűjtés és adatkezelés vonatkozásában. A biometrikus adatok közvetlen kapcsolata egyes „bizalmas" testi, illetve fiziológiai jellemzőkkel, mint például a betegségek vagy a faji eredet, illetve más, az intimszférába tartozó sajátosságok alapul szogálnak arra, hogy az Avtv. és más jogszabályok külön előírásokat rögzítsenek rájuk vonatkozóan. Az áttekintett nemzetközi és a szupranacionális szabályozás mellett a kelet-közép-európai új demokráciák közül számos állam integrált a biometrikus adatokra vonatkozó új fogalom-meghatározásokat és előírásokat korábbi adatvédelmi rendszerébe.[185] Ezek a megoldások zsinórmértéket jelenthetnének a magyar szabályok kialakításához is.

Az Avtv. mellett az adatvédelem ágazati szabályozása körében is számos jogszabály érinti a biometrikus adatok körét, egyik sem határozza azonban meg a biometrikus adatok fogalmát, vagy alkalmaz speciális előírásokat ezekkel az adatokkal összefüggésben. Az egyetlen kivételt a külföldre utazásról szóló 1998. évi XII. törvény jelenti, amelynek célja többek között a 22525/2004/EK Rendelet végrehajtása.

III. Technikai megfontolások

Technikai problémák leginkább a biometrikus adatok gyűjtésével, tárolásával és feldolgozásával, valamint az azonosítás és ellenőrzés folyamatával kapcsolatban merülnek fel. A biometrikus adatokat tartalmazó adatbázisok létrehozása és puszta léte is lehetővé teheti az állam és szervei számára, hogy az egyént ellenőrzésnek vessék alá. Mindemellett az adatok tárolására használt számítógépes rendszerek érzékenyek lehetnek a feltörésre és jogosulatlan felhasználásra. Szigorúan statisztikai szempontot alkalmazva, minél nagyobb az adatbázis, annál nagyobb a kockázata a személyes adatok jogosulatlan kezelésének. A biometrikus adatok gyűjtése és feldolgozása az adatkezelés egyik legfontosabb elvének, az átláthatóságnak a követelményével kerül ellentmondásba, egyrészt azért, mert biometrikus adatok, nyomok véletlenül is hagyhatók mindennapos használati tárgyakon, amely lehetővé teszi az egyén mozgásának és tevékenységének követését. Másrészt az RFID chipen keresztül lehetséges adatszerzés szintén lehetővé teszi az adatok jogosulatlan megszerzését.[186]

Az azonosítási/ellenőrzési folyamat során felmerülhet továbbá az a probléma, hogy az eljárás sosem rendelkezik százszázalékos pontossággal, két lehetséges hibája a téves azonosítás és a téves elutasítás. A hibák száma függ attól, hogy milyen pontossági küszöböt követelnek meg az azonosítás során. Ezt a küszöböt a rendszer működtetői határozzák meg, amely – kellő biztosítékok híján – önkényes is lehet, illetve lehetséges, hogy nem azonos az

[185] Vö. pl. a cseh adatvédelmi törvénnyel (2000. évi 101. törvény), a szlovák adatvédelmi tövénnyel (428/2002. törvény), továbbá a lengyel úti okmányokról szóló törvénnyel (2006. július 13-i törvény).
[186] Hornung: i. m.

egyes államokban, illetve azonosító rendszerekben, amely szintén problémákhoz vezethet. Több érv szól amellett, hogy az egyén meghatározott „részének" (jelen esetben a digitalizált, tárolt és azonosításra használt biometrikus adatnak) az identitás egészével való azonosítása felszámolja azt a teret, amelyet fizikális valónk és személyes identitásunk között rendszerint érzünk. Jelenleg bárki számára fennáll a lehetőség, hogy szükség esetén megváltoztassa személyes identitását (pl. tanúvédelmi program keretében). Ez nehezebbé vagy akár teljesen lehetetlenné is válhat, ha a személyazonosságot teljesen a fizikai megjelenéssel azonosítják.[187]

Végül, de nem utolsó sorban említést érdemel az a tényező, hogy adott célra begyűjtött biometrikus adat az egyén beleegyezése nélkül is felhasználható lesz más célokra. Pontos és szigorú előírások nélkül az összegyűjtött információ korlátlan számú tevékenységre lesz felhasználható. Természetesen ez a veszély a nem biometrikus személyes adatok esetében is fennáll, csak azért érdemel említést, mert a hagyományos személyes adatok sokszor kevésbé szenzitívek, illetve az azokra vonatkozó szabályok pontosabban meghatározottak és kezelésük nagyobb múltra, ennél fogva nagyobb gyakorlatra tekint vissza.

Záró megjegyzések

A terrorizmus elleni harcot, valamint az Európai unión belüli biztonság és jogszerűség fejlődését figyelembe véve valószínűsíthető, hogy az elkövetkezendő években a védelmi intézkedések száma és szigorúsága egyaránt növekedni fog. Akár ennek előnyeit, akár hátrányait hangsúlyozzuk, kétségtelen, hogy Magyarországnak teljesítenie kell azokat a feladatokat, amelyeket a nemzetközi, illetve szupranacionális dokumentumok, szabályok jelölnek ki számára. Mindez az jelenti, hogy megfelelő jogi kereteket, a biometrikus adatok kérdését explicit módon megjelenítő normákat kell beépíteni a magyar adatvédelmi jog rendszerébe. Számos, hasonló történelmi múlttal rendelkező kelet-közép-európai állam jogrendszere megfelelő példát és megoldási alternatívákat nyújt, azt jelezve, hogy a szupranacionális elvek implementálásának kihívásai kezelhetők.

A biometrikus azonosítók megfelelő integrálása a magyar rendszerbe azt kívánja, hogy ezek fogalma szerepeljen az Avtv.-ben, továbbá, hogy megvalósuljon egyes biometrikus azonosítók különleges adatként való meghatározása, tekintettel ezek közvetlen kapcsolatára az egyén intimszférájához tartozó vonásokkal. Az Avtv. háttér-előírásai mellett más, ágazati normákban is szükséges utalni a biometrikus adatokra. A szabályozási követelmények mellett fontos, hogy a biometrikus adatok felhasználásának kérdései eljussanak a közvéleményhez, lehetőséget nyújtva ezzel a társadalom tagjainak és szerveződéseinek, hogy kifejtsék álláspontjukat a problematikus kérdéskörökkel kapcsolatban.

[187] Vö. Biometrics at the Frontiers.