MYKOLO ROMERIO UNIVERSITETO
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETO
INFORMATIKOS IR STATISTIKOS KATEDRA

AURIMAS SAVICKAS
INFORMATIKOS TEISĖ

TEMA

# BIOMETRIJA IR ASMENS DUOMENŲ APSAUGA: TEISINIAI ASPEKTAI

Magistro baigiamasis darbas

**Darbo vadovas –**
**Doc. Dr. Darius Štitilis**

Vilnius, 2007

TURINYS

# Įvadas

**Temos aktualumas.** Tragiški 2001 m. rugsėjo 11 d. įvykiai[1], auganti terorizmo grėsmė, didėjantys nelegalios migracijos ir su ja susijusio nusikalstamumo srautai bei mažėjantis tradicinių migracijos valdymo ir asmenų identifikavimo priemonių patikimumas sąlygojo naujus iššūkius migracijos politikos srityje. Šių tendencijų kontekste, ieškant atsako į pastaruosius iššūkius, viena pagrindinių priemonių tampa naujų technologijų, visų pirma informacinių ir biometrinių, naudojimas asmens identifikavimui.

XXI a. pradžios saugumo iššūkiai paskatino naujų asmens identifikavimo metodų taikymą bei politines ir akademines diskusijas dėl asmens biometrinių duomenų naudojimo, kaupimo ir saugojimo metodų suderinamumo su jau išplėtotais žmogaus teisių standartais. Sparti biometrinių technologijų plėtra ir jų taikymas bei biometrinėms technologijoms teikiama politinė svarba[2] reikalauja atidaus jų nagrinėjimo duomenų apsaugos požiūriu. „Platus ir nekontroliuojamas biometrinių duomenų naudojimas kelia susirūpinimą asmenų pagrindinių teisių ir laisvių apsaugos atžvilgiu. Šie duomenys yra ypatingi, nes yra susiję su asmens elgsenos ir fiziologinėmis ypatybėmis bei įgalina jį ar ją individualiai identifikuoti.“[3]

Temos aktualumas apibrėžia ir **tyrimo objektą** – teisines biometrinei asmenų identifikacijai naudojamų asmens duomenų apsaugos problemas. Tyrimo objektas skiriamas į dvi pagrindines dalis – konkrečių biometrinių duomenų naudojimo identifikacijai (kaupimas ir saugojimas asmens identifikavimo priemonėse bei centrinėse ar vietinėse duomenų bazėse) reikalingumą ir pagrįstumą bei surinktų biometrinių asmens duomenų saugumą.

Biometrijos naudojimo asmens identifikavimui tema yra sąlyginai nauja kol kas nedaug nagrinėta. Todėl rengiant darbą buvo naudojamasi įvairiais šaltiniais. Pirmasis jų – jau priimti tarptautiniai, Europos Sąjungos ir atskirų nacionalinių valstybių teisės aktai, reglamentuojantys šių technologijų naudojimą. Antroji šaltinių grupė – įvairių formalių darbo grupių, nevyriausybinių organizacijų bei neformalių ekspertų forumų nuomonės ir rekomendacijos. Trečioji ir kol kas negausiausias šaltinių grupė – teisės ir biometrijos technologijų ekspertų nuomonės bei analitiniai darbai.

[1] Rugsėjo 11 d. teroristiniai išpuoliai JAV 2001 m., kuriuos surengė teroristinė grupuotė "Al Qaeda“. Per kelias valandas teroristai įvykdė tris sėkmingus pasikėsinimus: į Pasaulio prekybos centro pastatus ir Gynybos departamentą.
[2] Nuo 2001 m. rugsėjo 11 d. biometriniai duomenys dažnai vadinami geromis visuomenės saugumo priemonėmis.
[3] Direktyvos 95/46/EB 29 str. darbo grupės 2003 m. rugpjūčio 1 d. darbinis dokumentas (EN) Nr. 12168/02 „Darbinis dokumentas dėl biometrinių duomenų“// http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm ; Prisijungimo laikas: 2007-08-29.

Pirmoji šaltinių grupė apima nuo devintojo dešimtmečio pradėtus rengti tarptautinius susitarimus,[4] kuriuose buvo suformuotos asmens duomenų apsaugos politikos užuomazgos. Be šių tarptautinių organizacijų iniciatyvų asmens duomenų apsaugos bei biometrijos raidai turėjo ir atskirų valstybių teisinė praktika, kuriant biometrinių technologijų naudojimo standartus. Greta atskirų biometrijos reglamentavimo pavyzdžių, iš esmės didžiausios apimties analitinis ir teisės aktų rengimo darbas biometrijos naudojimo srityje yra atliekamas Europos Sąjungoje. Įgyvendinant iš bendrosios tarptautinės teisės prisiimtus žmogaus teisių apsaugos įsipareigojimus[5], ES nuo 1995 m. kuria technologijų vystymąsi atitinkančią teisinę bazę. Šiame kontekste pagrindinis vaidmuo tenka vienam iš patariamųjų ekspertinių prie ES Tarybos įkurtų komitetų - Direktyvos 95/46/EB 29 straipsnio Darbo grupei asmenų apsaugai tvarkant asmens duomenis (29 straipsnio grupei), rengiančiai ne tik rašytinės, bet ir biometrinės informacijos naudojimą asmens dokumentuose (skaitmeninis veido atvaizdas ir pirštų antspaudai) reglamentuojančių teisės aktų projektus.

Greta pirminių šaltinių svarbus vaidmuo biometrijos plėtros srityje tenka įvairiems ekspertų forumams bei netgi atskiroms kompanijoms, dirbančioms biometrijos srityje. Vienas svarbiausių ekspertų forumų - Tarptautinė biometrijos grupė, susikūrusi dešimtojo dešimtmečio pabaigoje, jau yra tapusi svarbia konsultacine institucija, teikiančia rekomendacijas ir pasaulio valstybėms.

Daugelyje Vakarų šalių šiuo metu vyksta diskusija dėl biometrinių duomenų dokumentuose patikimumo, efektyvumo ir svarbiausia – dėl jų įtakos asmens teisei į privatų gyvenimą. „Neaišku, ar įtraukus biometrinius identifikuojamuosius duomenis į dokumentus iš tikrųjų sustiprės saugumas, o galbūt priešingai kils grėsmė saugumui dėl piktnaudžiavimo rizikos, technologijų paklaidų ir skaidrumo bei solidžios duomenų apsaugos trūkumo.“[6] Be to, pačių biometrinių standartų įdiegimas kartais siejamas ne tiek su technine būtinybe, kiek su politiniu spaudimu[7].

Biometrinių duomenų naudojimo problematika yra nedaug nagrinėta ir pasauliniu mastu. Mažiausiai yra nagrinėtas šio klausimo normatyvinis aspektas. Kiek plačiau yra išnagrinėti

---

[4] Pavyzdžiui, Europos Tarybos konvencija dėl Asmenų apsaugos automatiškai apdorojant asmens duomenis (1981 m.), Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) Asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairės (1980 m.) ir kt.

[5] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:006:LT:HTML; Prisijungimo laikas: 2007-11- 10 įžanginė citata, 1992 metų Europos Sąjungos Sutartis (Mastrichto sutartis) // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=32156 ; Prisijungimo laikas: 2007-11-15.

[6] Europos Sąjungos Piliečių laisvių, teisingumo ir vidaus reikalų komiteto pranešimo projektas Nr. PE 349.798 „Pasiūlymas dėl Tarybos reglamento dėl ES piliečių pasų saugumo priemonių standartų ir biometrikos“, 2004.10.14.

[7] Asta Radvilaitė, Žmogaus teisių stebėjimo instituto tyrimų atstovė, teigia, kad „Europos Sąjungai buvo primesti Tarptautinės civilinės aviacijos organizacijos, kuri yra niekam neatskaitinga, nedemokratiniu būdu sukurti biometrinių pasų standartai. Nebuvo atsižvelgta nei į ekspertų, nei į Europos Parlamento nuomonę dėl tokių pasų keliamo pavojaus privatumui. Reglamente nėra tinkamai paaiškinta, kokia yra biometrinių duomenų įtraukimo į pasus būtinybė, nėra informacijos apie jų patikimumą, veiksmingumą ir svarbiausia - nėra išlaikytas proporcionalumo principas, nes biometrinių pasų keliama rizika asmens privatumui yra pernelyg didelė, o patikimumas mažas.“

techniniai, politiniai ir ekonominiai šio klausimo aspektai. Teisiniu aspektu aptariamą temą gvildeno labai maža dalis autorių, todėl didžiausias informacijos šaltinis rašant šį darbą buvo informacija internete. Darbas parengtas daugiausiai vadovaujantis užsienio šalių autorių darbais. Paminėtini C. Prins, C. Guerrier, Paul de Hert, R. Clarke, J. D. Woodward, A. Ashbourn.

Lietuvoje diskusija dėl biometrinių duomenų patikimumo beveik nevyksta, dėl to visuomenė nėra tinkamai informuojama apie biometrinių pasų patikimumą, efektyvumą ir svarbiausia - apie jų įtaką asmens teisei į privatų gyvenimą. Iki šiol nėra žinoma Valstybinės duomenų apsaugos inspekcijos nuomonė minėtais klausimais, o, anot H.Mickevičiaus, Žmogaus teisių stebėjimo instituto direktoriaus, „visuomenės informavimas yra panašus į viešųjų ryšių akciją ar reklamos kampaniją, kurioje biometrinių pasų įvedimas yra pristatomas tik kaip patraukli, piliečių saugumą didinanti technologinė naujovė“[8]. Nagrinėti biometrinių technologijų taikymo Lietuvoje teisinius aspektus nėra lengvai įgyvendinama užduotis ir todėl, kad ši sritis mažai reglamentuota nacionaliniais teisės aktais, yra menkai nagrinėta akademinėje literatūroje, retai aptariama net ir šioje srityje veikiančių institucijų techniniuose dokumentuose. Savo ruožtu, atsižvelgiant į Lietuvos, kaip ES narės įsipareigojimus, perimti ir įgyvendinti visą *acquis communautaire*, šį informacijos vakuumą iš daleis galima kompensuoti analizuojant atitinkamus teisinius ir akademinius ES lygmens dokumentus.

Šios problemos bei temos naujumas ir paskatino rašyti magistro baigiamąjį darbą šia tema ir tuo pačiu gilintis į asmens duomenų apsaugos ir biometrijos problematiką, siekiant įvertinti Europos Sąjungos valstybių narių ir kitų šalių asmens duomenų apsaugos ir biometrijos teisinę bazę bei identifikuoti pagrindines šios srities problemas.

Pagrindinis šio **darbo tikslas** – išanalizuoti teisinius biometrinių duomenų naudojimo aspektus bei jų sąsajas su duomenų apsaugos reikalavimais, identifikuoti pagrindines problemas, įvertinti šios srities būklę, plėtros kryptis ir tokiu būdu sudaryti prielaidas tolimesniems išsamesniems tyrimams Lietuvoje. Šiai temai atskleisti naudojamasi ES valstybių narių išduodamų piliečių pasų teisinio reglamentavimo analizė, nes būtent nemaža dalimi išorės jėgos sąlygotas biometrijos taikymas šiuose pagrindiniuose asmens tapatybės dokumentuose nuo dešimtojo dešimtmečio vidurio sąlygojo ekspertų diskusijos bei biometriją reglamentuojančių teisės aktų atsiradimą.

Siekiant darbo tikslo, keliami šie **uždaviniai:**

1. Aptarti naudojamas biometrinių duomenų technologijas ir jų sąlygojamas grėsmes asmens privatumui.

[8] Mickevičius H. Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą, Žmogaus teisių stebėjimo institutas. 2006 // http://www.hrmi.lt/news.php?strid=1999&id=3455; Prisijungimo laikas: 2007-08-29.

2. Surinkti bei susisteminti informaciją apie teisinę ir techninę su biometrinių technologijų naudojimu susijusią asmens duomenų apsaugos problematiką.
3. Išanalizuoti ir įvertinti svarbiausius Europos Sąjungos ir tarptautinės teisės aktus, reglamentuojančius asmens duomenų apsaugą biometrinių duomenų naudojimo kontekste (kadangi Lietuvoje priimti teisės aktai asmens duomenų apsaugos srityje iš esmės atkartoja ES teisės aktų nuostatas, jie nebus nagrinėjami atskirai), įskaitant teisinę bazę, reglamentuojančią biometrinių duomenų naudojimą vieno pagrindinių asmens identifikavimo dokumentų – Europos Sąjungos valstybių narių piliečių pasuose;
4. Pateikti išsamų problemų, susijusių su asmens duomenų apsauga biometrijoje, sąrašą ir tokiu būdu sudaryti pagrindą tolimesnėms studijoms aptariamoje srityje.

Analizuojant asmens duomenų apsaugos problematiką biometrijos naudojimo kontekste taikomi šie **tyrimo metodai**: nagrinėjant asmens duomenų apsaugos ir biometrijos sampratas taikomas *istorinis metodas*; analizuojant asmens duomenų apsaugos ir biometrijos reglamentavimo ypatumus ES valstybėse narėse ir kitose šalyse naudojamas *kontent-analizės* ir *lyginamosios analizės* metodai.

Skaitant šį darbą vietomis gali kilti įspūdis, jog daug dėmesio yra skiriama ne vien teisiniam, bet ir techniniam problemos aspektui. Autoriaus nuomone, tai neišvengiama dėl biometrinių technologijų specifikos – jų techninio pobūdžio. Atsižvelgiant į tai, techninės tematikos terminologija bus neišvengiamai naudojama ne tik pavyzdžiuose ar situacijų aprašymuose, bet ir analizuojant teisės normas.

# I. Biometrijos samprata

## *1. Biometrijos sąvokos*

Terminas „biometrija“ yra kildinamas iš graikų kalbos žodžių „*bios*“ (gyvybė) ir „*metron*“ ar „*metrikos*“ (matas). Ilgą laiką „biometrija“ buvo suprantama, kaip statistikos metodų panaudojimas biologinių tyrimų apdorojimui[9]. Panašiai sąvoka aiškina ir kompiuterinis tarptautinių žodžių žodynas „Interleksis“ – t.y., biologinių tyrimų planavimo ir duomenų apdorojimo matematinės statistikos metodais būdų visumą. Ši „netechnologiška“ sąvoka, dar vadinama biologine statistika, dažniausiai naudojama medicinoje, biologijoje, agronomijoje ir farmacijoje.

Aštuntajame praeito amžiaus dešimtmetyje, informacinių technologijų vystymosi bumo metu asmens tapatybei nustatyti pradėjus taikyti automatines technologijas, kurių pagalba pradėta vertinti ir analizuoti žmogaus fiziniai ir elgsenos bruožai, terminas „biometrija“ įgavo papildomą reikšmę. „Biometrija“ suprantama, kaip „asmens atpažinimas automatinių metodų pagalba, analizuojant žmogaus fiziologinės ir elgesio ypatybės.“[10] Būtent, pastarąja reikšme ir bus remiamasi šiame darbe. Reikia pažymėti, kad teisinės termino „biometrija" reikšmės kol kas dar nėra sukurta[11].

Biometrinėse technologijose asmens identifikavimui paprastai naudojamas vienas arba kelis pagrindiniai unikalūs žmogaus bruožai: piršto atspaudas, veido bruožai, akies rainelė, balsas, rečiau naudojami kiti fiziologiniai (delno atspaudas, akies tinklainė) arba elgesio (parašo skanavimas, klavišų spaudimo skanavimas) parametrai.[12] Toliau pateikiamos keletas su biometrija ir biometrinėmis technologijomis susijusių sąvokų, kurios palengvins biometrijos, kaip sąvokos, ir biometrinių technologijų suvokimą ir bus naudojamos šiame darbe.

**Biometrinės savybės / charakteristikos** (angl. *biometric characteristics*) – tai išmatuojamos elgsenos ir fiziologinės ypatybės, naudojamos asmens atpažinimui. Biometrinės charakteristikos (ypatybės) gali būti *fiziologinės* arba *elgesio*[13]. Fiziologinės (pasyvios) ypatybės yra parametrai, kuriuos galima išmatuoti ant tam tikros kūno dalies, tam tikru momentu. Tuo tarpu kitos, kurios yra išmoktos ar įgyjamos per tam tikrą laiką, vadinamos elgesio savybėmis (aktyvios). Pastarosios yra

[9] Shorter Oxford English Dictionary: Sixt Edition . Oxford University Press, 2006.
[10] The Biometric Contortium.. Intro to biometrics // http://www.biometrics.org/intro.htm; Prisijungimo laikas: 2006-11-06
[11] Guerrier C., Cornelie L-A, Les aspects juridiques de la biometrie, http://www.biometrie-online.net/dossiers/generalites/droit/Claudine%20GUERRIER.pdf; Prisijungimo laikas; 2007-10-17 . .
[12] Nanavati S, Thieme M, Nanavati R, Biometrics. Identity Verification in a Networked World. New York: A Wiley Tech Brief Wiley Computer Publishing, 2002. P. 43-139
[13] Miller B. Vital signs of identity.// IEEE Spectrum: Vol. 31, No. 2, 1994.

sukuriamos žmogaus ypatingų pastangų dėka ir dėl to jos yra tam tikru laipsniu priklausomos nuo jo proto būsenos.

Pagal šiuos apibrėžimus, pirštų atspaudai, rankos geometrija, veidas yra fiziologinės biometrinės ypatybės, tuo tarpu dinaminis parašas, eisena, klavišų spaudimo dinamika, taip pat lūpų judesiai yra elgesio biometrinės ypatybės. Pažymėtina, kad balsas gali būti nagrinėjamas, kaip fizinių ir elgesio ypatybių derinys. Balsas skiriamas tiek prie fiziologinių ypatybių – dėl balso stygų vibracijos ir burnos formos, tiek ir prie elgesio ypatybių - dėl kalbančio žmogaus proto būsenos.

Kalbant apie biometrines charakteristikas yra išskiriama dar viena grupė – *biologinės*[14]. Prie pastarųjų yra priskiriama deoksiribonukleo rūgšties (DNR) molekulė. Tiriant kraują, išskyras, plaukus, audinius yra patikrinamas tiriamo objekto DNR struktūros sutapimas su konkrečių asmenų DNR struktūromis ir nustatoma tiriamo objekto priklausomybė identifikuojamam asmeniui.

**Biometrinis atvaizdas** (angl. *biometric sample*) – biometrinės sistemos užfiksuota, dar neapdorota („žalia“) informacija su duomenų subjekto biometrinėmis ypatybėmis.

**Biometriniai duomenys** (angl. *biometric data***)** – apdorota biometrinio pobūdžio informacija, panaudota informacijos davėjo biometriniam modeliui sukurti.

**Biometrinis modelis** (angl. *biometric template*) - savarankiška matematinė informacijos aibė, išskaičiuota iš biometrinio atvaizdo. Modelis yra biometrinio atvaizdo struktūrinis sumažinimas, t.y., užfiksuoti individo biometriniai matmenys.

**Biometrinė sistema** – biometrinių technologijų pritaikymas, kuris leidžia automatiškai identifikuoti (nustatyti asmens tapatybę) ir/ar autentifikuoti/verifikuoti[15] asmenį

Šiame darbe sąvoka **biometrinėmis technologijomis** bus laikomi visi kompiuterinėmis sistemomis paremti metodai (angl. *computer-based methods*), kurie remdamiesi biometrinėmis ypatybėmis atpažįsta žmones.

**Biometrinis skanavimas** yra procesas, kuriuo biometrinės duomenys yra surenkami ir registruojami kompiuterinėje sistemoje, turint tikslą patikrinti arba nustatyti asmens tapatybę. Biometrinę apsaugos sistemą sudaro jutiklis matuojamo objekto atvaizdui įvesti ir kompiuteris su specialia atvaizdo identifikavimo programa bei duomenų bazė, kurioje saugomi anksčiau įvestų atvaizdų aprašymai.

[14] Miller B. Vital signs of identity.// IEEE Spectrum: Vol. 31, No. 2, 1994.
[15] Apie identifikavimo (asmens tapatybės nustatymo) ir autentifikavimo/verifikavimo skirtumą bus rašoma žemiau.

## *2. Biometrinės sistemos*

Biometrinių technologijų taikymas, nepriklausomai nuo naudojamų duomenų tipo, susideda iš dviejų etapų: *biometrinių duomenų registracijos* ir *biometrinių duomenų palyginimo (sugretinimo).* Registracijos metu biometriniai duomenys yra užfiksuojami ir perkeliami į biometrinį modelį, kuriame yra įrašyta unikali biometrinė informacija. Toks biometrinis modelis yra užfiksuojamas duomenų bazėje. Biometrinių duomenų palyginimo (sugretinimo) metu yra nuskaitomas naujas pavyzdys iš „gyvos“ biometrinės informacijos, ir tas pavyzdys suformuoja palyginimo modelį, kuris yra sugretinamas su pirmiau sukurtu modeliu, kuriame yra pirminės registracijos metu gauta biometrinė informacija.

Biometrinis modelis, sukurtas iš neapdorotos biometrinės informacijos, paprastai sukelia diskusijų apie privatumą dėl tokios informacijos saugojimo proceso. Apskritai biometrinis modelis (pavyzdžiui, piršto antspaudas) pats savaime nėra neapdorota informacija. Jis yra išgaunamas po tam tikros neapdorotos informacijos biometrinių duomenų analizės ir apibendrinimo. Visa tai tik dalis biometrinės informacijos, kuri, kaip teigiama literatūroje, yra neatstatoma, kas reiškia, jog neapdorotos biometrinės informacijos (pvz. piršto antspaudo) negalima „atgauti atgal“, t.y. lyg ji nebūtų buvusi paimta iš biometrinio modelio.

Kiekvieno asmens biometrinis modelis yra laikomas unikaliu, kaip ir pati neapdorota biometrinė informacija, ir jis yra informacijos apie biometrinio modelio savininką identifikatorius (originalas) su kuriuo bus lyginami visi vėliau sukaupti duomenys.

Taigi, biometrinio modelio saugojimas nėra pažangesnis už neapdorotą (žalią) biometrinę informaciją. Neįslaptintas biometrinis modelis gali būti lengvai pažeidžiamas, ko pasekoje gali būti patenkama į sistemą (naudojant saugumo kodą) ir identifikuojamas vartotojas. Tačiau, taip pat nėra šimtaprocentinės garantijos, kad modeliai nebus kokiu nors būdu atkurti.[16]

Žvelgiant iš teisinės perspektyvos, visos biometrinės technologijos Europos Sąjungoje yra reglamentuotos 1995 m. spalio 24 d. direktyva 95/46/EB „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo”, nes biometrinis apdorojimas apima „būdus

[16] Naudojant daugiapakopes atakas (angl. *hill-climbing atack*) tam, kad atkurti neapdorotą (žalią) informaciją pakartotinio apdorojimo būdu kai kurie duomenys gali būti perdaryti. // Adler A., Images Can Be Regenerated From Quantized Biometric Match Score Data. 2004 // http://www.sce.carleton.ca/faculty/adler/publications/2004/adler-2004-ccece-quantized-match-score.pdf; Prisijungimo laikas: 2007-10-17.

surinkti, persiųsti, manipuliuoti, įrašyti, saugoti ar perduoti su fiziniais asmenimis susijusius garsinius ir vaizdinius duomenis“ [17].

Reziumuojant šioje darbo dalyje išdėstytą informaciją akcentuotina tai, kad biometriniai duomenys yra gaunami iš asmens ir yra naudojami patikrinti ar nustatyti asmens tapatybę. Biometriniai duomenys yra ypatingos išskirtinės asmens psichologinės, elgesio ar biologinės savybės. „Asmens duomenų“ sąvoka, kaip apibrėžta Direktyvoje 95/46/EB, apima tiek neapdorotus biometrinius duomenis, tiek biometrinį modelį.

## *3. Privatumas biometrijos kontekste*

### 3.1. Privatumo samprata

Informacinių technologijų ir biometrijos kontekste „privatumo“ ir „informacijos kontrolės“ sąvokos turi daug panašumų. Privatumo sąvoką apibrėžiant per informacijos sklaidą „privatumas yra asmens, grupių ar institucijų pretenzija nusistatyti kada, kaip ir kokia apimtimi informacija apie juos gali būti perduodama kitiems“[18]. „Pagrindinis privatumo teisės požymis – asmens gebėjimas kontroliuoti informacijos apie jį patį platinimą“[19]. Elgesem pateikia tokią privatumo sampratą: „turėti asmeninį privatumą – tai galimybė turėti leidimą platinti asmeninę informaciją“.[20] Biometrijos kontekste, informacinis privatumas arba informacijos apie save kontroliavimas, yra vienas esminių privatumo klausimų, kurį iškėlė ši nauja technologija. Asmenys yra suinteresuoti, kad būtų nustatyta kada, kodėl ir kam informacija apie juos bus atskleista per biometrinius identifikatorius[21].

Visgi, privatumas susideda ne vien iš informacijos privatumo. Tarptautinių teisės aktų analizė leidžia daryti išvadą, kad asmens teisės į privatumą turinį sudaro keturi savarankiški ir kartu tarpusavyje susiję elementai: a) *informacinis privatumas* - susijęs su duomenų apie asmenį tvarkymu ir vadinamas asmens duomenų apsauga; b) *fizinis privatumas* (kūno neliečiamumas), t.y. nesant žmogaus sutikimo, jo atžvilgiu negali būti atliekami jokie medicininiai ar moksliniai

[17] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, 14 įžanginė citata.

[18] Bier W. C., Right of Privacy. Fordham University Press, 1980. P. 196 // http://books.google.com/books?id=rofFPZc0nooC&pg=PA196&dq=%22%22; Prisijungimo laikas: 2007-10-17.

[19] Ten pat.

[20] Elgesem D. Privacy, Respect for Persons, and Risk // Charles Ess, Philosophical Perspective on Computer Mediated Communication. New York State University of New York Press, 1996. P. 51 // http://books.google.com/books?id=5IvvWDXBcakC&dq=%22; Prisijungimo laikas: 2007-10-17

[21] John D. W. Biometrics: Identifying Law &Policy Concerns in Biometrics // Anil Jain ir kt. Personal Identification in Networked Society.// http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf.; Prisijungimo laikas: 2007-10-17.

bandymai (pavyzdžiui, privaloma tvarka paimamas DNR mėginys ir pan.); c) *komunikacinis privatumas,* - asmens susirašinėjimo, pokalbių telefonu, telegrafo pranešimų ir kitokio susižinojimo neliečiamumas; d) *teritorinis privatumas,* - asmens būsto arba teritorijos neliečiamumas.[22]

Atsižvelgiant į šį teisinį reglamentavimą, informacijos kontrolės sąvoka nėra tinkamiausias privatumo apibrėžimas. Šiame kontekste „privatumo“ sąvoką tikslinga apibrėžti vadovaujantis R.Gavison pateikta sąvoka, kaip „ribotą prieinamumą“[23], kuris, savo ruožtu, susideda iš trijų susijusių, bet nepriklausomų sudėtinių elementų: *slaptumo*, *anonimiškumo* ir *vienatvės*.

- **Slaptumas**[24] (asmens teisė bendrauti su paties pasirinktais asmenimis, nepatiriant išorinio kišimosi) - ši sąvoka atrodo daug tinkamesnė už aukščiau minėtą „informacijos kontrolės“ sąvoką. Ji nenustato galimybės pasirinkti, ar atskleisti ir kokia apimtimi atskleisti informaciją apie save kitiems, bet atskleidžia tikrąją situaciją apie informacijos paviešinimą, t.y. kai kiti asmenys siekia informacijos apie mus, mes netenkame savo privatumo.
- **Anonimiškumas** (asmens teisė išlikti neatpažintam)[25] gali būti naudingas kaip atspirties taškas kuriant privatumą, bet jo neužtikrina[26]. Kai asmens tapatybė yra atskleidžiama ir anonimiškumas pažeidžiamas, tikėtina, kad yra pažeidžiamas ir privatumas. Reikia pažymėti, kad praktikoje, daugumos privatumą skatinančių technologijų (angl. *privacy enhancing technologies*) tikslas yra stiprinti privatumą užtikrinant anonimiškumą.[27]
- **Vienatvė** (asmens teisė nebūti stebimam) - biometrijos kontekste nuošalumas yra suvokiamas kaip privatumo aspektas, susijęs su asmens kūno integralumu (vientisumu)[28]. Integralumo sąvoka apibrėžiama asmens teisė į jo neliečiamumą, harmoningą funkcionalumą, paremtą informacijos ieškančio asmens pagarba asmeniui apie kurį yra ieškoma informacijos. Biometrijos kontekste nuošalumo principas gali būti aktualus, kai yra atliekamas priverstinis pirštų antspaudų ar DNR mėginių paėmimas.

[22] Žr. Visuotinės žmogaus teisių deklaracijos 12 straipsnį, Tarptautinio pilietinių ir politinių teisių pakto 17 straipsnį, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnį ir kt.
[23] Gavison R.. Privacy and the Limits of the Law // Yale Law Journal. Vol. 89, No. 3. Jan, 1980. P. 428.
[24] Jis nurodo apie galimą privatumo netekimą, kai kiti išgauna informaciją apie asmenį.
[25] H.Nissenbaum teigia, kad supratimas apie prigimtinę privatumo reikšmę lieka neapibrėžtas. Bet yra neginčijama tai, kad anonimiškumo reikšmė kompiuterizuotame pasaulyje nelieka neapibrėžta, o anonimiškumas yra kaip galimybė asmeniui veikti ar dalyvauti kai asmuo nėra pasiekiamas // Nissenbaum H. The Meaning of Anonymity in an Information Age. // The Information Society, Nr.15. 1999. P. 141.
[26] Custers B.H.M. The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Tilburg: Wolf Legal Publishers, 2004. P. 172.
[27] Hes R., Borking, T., Privacy Enhancing Technologies: The Path to Anonymity. Hague: Registratiiekamer, 1998 // http://66.102.1.104/scholar?q=cache:WEeBHFbtzEMJ:www.cbpweb.nl/documenten/av_11_Privacy-Penhancing_technologies.html; Prisijungimo laikas: 2007-10-17.
[28] Bloustein E. J. Privacy as an Aspect of Human Digni: An answer to Dean Prosser. // New York University Law review, 1964. P. 39.

Privatumo saugojimas atitinka daug svarbių vertybių ir interesų. Privatumas apsaugo individualumą[29]. Privatumas yra unifikuota ir nuosekli koncepcija, apsauganti nuo elgesio, kuris žeidžia asmens orumą ar kėsinasi į žmogaus asmenybę[30]. Privatumas gali būti pažeistas, netgi tokiu atrodo nekaltu įsibrovimu, kaip stebėjimas. Akivaizdu, kad yra „būdų įžeisti asmens orumą ir asmenybę, kurie neturi nieko bendro su privatumu“[31]. Ši teorija nurodo, kodėl yra vertinamas privatumas – t.y. kaip individualumo, orumo ir autonomiškumo garantas. Biometrijos panaudojimas, kuris yra laikomas iš prigimties pažeidžiančiu asmens vientisumą ar orumą, gali tapti mažiau nepriimtinu, jeigu privatumo yra paisoma panaudojant biometrines technologijas.

## 3.2. Privatumas ir biometrinės sistemos

Daugiau nei dešimtmetį veikianti viena stambiausių biometrijos konsultacinių įmonių bei viena autoritetingiausių ekspertų grupių – Tarptautinė biometrijos grupė[32] nurodo esant nenutrūkstamą ryšį tarp biometrinės sistemos ir privatumo.[33] Wayman pažymi, jog biometrinių duomenų naudojimo galimybė sąlygoja visuomenės reikalavimus dėl informavimo šiuo klausimu.[34]. Šią problematiką analizuojančioje literatūroje biometrinių sistemų santykius su privatumu yra apibrėžiamas išskiriant keturis sistemų tipus:

- **Privatumą apsaugančios sistemos.** Sistema yra apsauganti privatumą, jeigu ji naudojama saugant arba ribojant priėjimą prie asmeninių duomenų arba jeigu ši sistema tarnauja kaip priemonė nustatant patikimą tapatybę (pvz., savininko sąskaitos verifikavimo sistemos).
- **Privatumui palankios sistemos.** Sistema yra palanki privatumui, jeigu ji naudojama su tam tikrais apribojimais arba jeigu sistema yra skirta užtikrinti apsaugą nuo neteisėto priėjimo prie duomenų ir jų naudojimo.
- **Privatumo atžvilgiu neutralios sistemos**. Sistema yra neutrali privatumo atžvilgiu, jeigu jos naudojimas privatumui turi nedidelį poveikį (pvz., asmeninių kompiuterių prieigos sistemos).

[29] Bloustein E. J. Privacy as an Aspect of Human Digni: An answer to Dean Prosser. // New York University Law review, 1964. P. 39.
[30] Ten pat.
[31] Gavison R. Privacy and the Limits of the Law // Yale Law Journal. Vol 89, No. 3. Jan, 1980. P. 438.
[32] Tarptautinės Biometrinės Grupės tinklapis: http://www.biometricgroup.com;
[33] The Bioprivacy Initiative: A Framework For Evaluating The Privacy Impact Of Biometric Deployment And Technologies. International Biometric Group (IBG), M1/03-0227, 2002. // http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/14-Bio-Privacy.pdf ; Prisijungimo laikas: 2007-09-12.
[34] Wayman J. L. ir kt. Biometric Systems: Technology, Design and Performance Evaluation. London: Springer-Verlag, 2005. P. 16.

- **Privatumą varžančios sistemos.** Sistema kėsinasi į privatumą, jeigu ja galima naudotis asmeniui nežinant, nesant jo sutikimo arba nenurodant naudojimosi sistema tikslų[35] (pavyzdžiui, kai kurios nacionalinės asmens tapatybės duomenų sistemos, sekimo sistemos).

J. Woodward pažymi, jog technologijų vystymasis neretai aplenkia jų naudojimą galinčio reglamentuoti teisinio reguliavimo būklę. Atitinkamai dėl naujų technologijų įdiegimo, atsižvelgiant į jų sąlygojamus iššūkius ir teikiamas galimybes, turi būti peržiūrima esama teisinė bazė arba rengiamas visiškai naujas reglamentavimas, kartu apibrėžiant visuomenei priimtinas ribas, taikomas naudojant naująsias technologijas. Būtent tai vyksta šiuo metu įdiegiant biometrinių duomenų naudojimą kasdienėje veikloje bei tapatybės dokumentuose. Teisės ekspertai, pasitelkdami technologijų ekspertus, privalo ištirti, „kas yra būtina siekiant apsaugoti viešąjį interesą ir užtikrinti visuomenei optimalius rezultatus“[36]. Kaip ir daugelio naujų technologijomis atveju, biometrinių technologijų naudojimas sąlygoja tam tikrų esminių probleminių klausimų:[37]

- **Nesankcionuotas biometrinių duomenų rinkimas.** Šiuo atveju akcentuotinos privatumui kylančios grėsmės, kai biometrinių technologijų pagalba renkama informacija to nežinant biometrinių duomenų subjektui.
- **Bereikalingas biometrinių duomenų rinkimas.** Grėsmė asmens privatumui iškyla tada, kai biometrinės technologijos yra naudojamos ten, kur tai nėra būtina bei pagrįsta[38].
- **Nesankcionuotas biometrinių duomenų naudojimas.** Nesankcionuotas biometrinių duomenų naudojimas sudaro didžiausią grėsmę biometrinių duomenų privatumui. Grėsmė kyla ne dėl iš anksto numatyto duomenų naudojimo, bet dėl būdų, kuriais jie gali panaudoti nenumatytiems tikslams. Nesankcionuoto duomenų naudojimo grėsmės gali būti skirstomos į grėsmes dėl daktiloskopinių duomenų naudojimo[39] ir biometrinių duomenų, kaip unikaliojo identifikatoriaus (pvz. asmens kodas) naudojimo nustatant asmenį tapatybę.

---

[35] The Bioprivacy Initiative: A Framework For Evaluating The Privacy Impact Of Biometric Deployment And Technologies. International Biometric Group (IBG), M1/03-0227, 2002. // http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/14-Bio-Privacy.pdf ; P. 2, Prisijungimo laikas: 2007-09-12.

[36] Woodward J. D. Biometrics: Privacy's foe or privacy's friend? // Proceedings of the IEEE, Nr. 9, 1997. P. 1480.

[37] Rosenzweig P., Kochems A., Schwartz, A. Biometric technologies: Security, legal, and policy implications. Legal Memorandum. 2004. // http://www.heritage.org/Research/HomelandSecurity/lm12.cfm; Prisijungimo laikas: 2007-10-17

[38] Jean Rostand koledže Nicoje patekimui į valgyklą buvo pasirinkta biometrinė duomenų bazė, automatiškai atpažįstanti susijusius fizinius asmenis pagal pirštų atspaudus. Tačiau Prancūzijos duomenų apsaugos komisija CNIL nepritarė dėl neproporcingumo tarp priemonių ir siekiamo pirminio tikslo.

[39] Grėsmės privatumui gali kilti tada, jeigu, pavyzdžiui, teisėsaugos institucijos pradėtų naudotis privačios kompanijos biometrine duomenų baze, kurioje saugomi asmenų, kurie gali patekti į patalpas, pirštų atspaudai.

- **Biometrinių duomenų, kaip unikalių identifikatorių, naudojimas.** Kadangi biometrinės technologijos remiasi asmens fiziologinėmis ir elgesio charakteristikomis ir tuo, kad šios charakteristikos (pvz. pirštų antspaudai) yra unikalios, kyla pavojus, kad biometriniai duomenys gali pasitarnauti kaip unikalūs identifikatoriai. Pavojus kyla tame, kad biometrinė informacija esanti „atsekamoje formoje“, t.y., kol ji yra „neapdorotame“ pavidale gali būti susieta su kitais asmens duomenimis.
- **Nesankcionuotas duomenų atskleidimas –** situacija, kai duomenų subjektas netenka galimybės kontroliuoti savo asmens duomenų naudojimo. Grėsmė netekti galimybės kontroliuoti savo asmeninės informacijos yra vieną opiausių problemų privatumo kontekste. Įtraukiant biometrinius duomenis į kokį nors projektą būtina saugotis nesankcionuoto duomenų atskleidimo sukuriant privatumą užtikrinančią sistemą ir procedūrinę apsaugą.
- **Funkcijų deformacija** (angl. *function creep*) atsiranda tada, kai asmens duomenys panaudojami kitiems tikslams, nei buvo numatyta iš anksto, arba kai biometrinės sistemos yra sureguliuotos susirinkti daugiau informacijos nei būtina.

Visų aukščiau paminėtų situacijų atsiradimą nulemia faktas, kad biometriniai duomenys, surinkti sistemos, gali būti susiję su asmenine informacija arba gali sudaryti sąlygas sekti asmens judėjimą[40]. J. Wayman ir kiti pabrėžia, kad šios naujos technologijos „gali susieti asmenį su biometriniu pavyzdžiu ir kitais tapatybės duomenimis, taip pat su asmeniniu priskyrimu užsiregistravimo sistemoje metu“[41] ir kad autentiškumo nustatymo anonimiškumas gali būti užtikrinamas tik tada, kai negali būti ryšio tarp biometrinių duomenų ir asmeninės informacijos.

Kaip jau buvo minėta anksčiau, biometrinių duomenų naudojimas yra saugiausias būdas patvirtinti tam tikro asmens tapatybę. Tačiau biometrinių sistemų naudojimas reikalauja, kad dėl galutinio tikslo būtų vadovaujamasi proporcingumo principu, atsižvelgiant į tinkamumo ir pagrįstumo kriterijus. Iš tiesų biometrinių sistemų naudojimo tikslas ir pavojai, kuriuos gali sukelti duomenų bazių struktūros ypatumai, turi būti proporcingi vieni kitiems.

Pažymėtina, kad bet kurios biometrinės sistemos įrengimo lygis nusako santykį tarp biometrinių duomenų ir privatumo[42]. Siekiant įvertinti kompiuterinių sistemų poveikį privatumo apsaugai, buvo sukurta keletas metodikų. Bendrą - „poveikio privatumui įvertinimo metodiką“, kuri

[40] Wayman J. L. ir kt. Biometric Systems: Technology, Design and Performance Evaluation. London: Springer-Verlag, 2005. P. 15.
[41] Ten pat. P. 16.
[42] International Biometric Group. The Bioprivacy Initiative: A Framework For Evaluating The Privacy Impact Of Biometric Deployment And Technologies. International Biometric Group (IBG), M1/03-0227, 2002 // http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/14-Bio-Privacy.pdf; Prisijungimo laikas: 2007-09-12.

gali būti taikoma biometrinių duomenų atveju tapatybės dokumentams, siūlo R.Clarke.[43] Šioje metodikoje siūloma 18 klausimų kategorijų (duomenų išsaugojimas, atskaitomybė, sutikimas ir kt.), kuriuos būtina užduoti siekiant sukurti naują sistemą.

Tarptautinė biometrijos grupė sukūrė metodologinę priemonę – klausimų rinkinį, skirtą įvertinti tam tikros biometrinės sistemos įrengimo lygį tam tikroje aplinkoje[44]. Pateikiamų klausimų tikslas yra išsiaiškinti, kokių tinkamų atsargumo ir apsaugos priemonių galėtų būti imamasi konkrečioje situacijoje. Kiekvienas klausimas apibūdina grėsmę, galinčią kilti privatumui:

1. Ar sistema yra įrengta viešai ar slaptai?
2. Ar sistema yra laisvai pasirenkama, ar privaloma?
3. Ar sistema naudojama autentifikavimui/verifikavimui ar identifikavimui?
4. Ar sistema yra įrengiama fiksuotam laikotarpiui, ar terminas nėra apibrėžtas?
5. Ar sistema įrengta privačiame ar viešajame sektoriuje?
6. Kokia yra sistemos vartotojo padėtis: ar jis veikia kaip asmuo/klientas ar kaip darbuotojas/pilietis?
7. Kas valdo biometrinius duomenis – asmuo, kuris registruojasi sistemoje ar institucija?
8. Kur saugomi biometriniai duomenys: asmeninėje atmintinėje[45] ar centrinėje duomenų bazėje?
9. Kokius biometrinius duomenis fiksuos sistema: elgesio ar fiziologines charakteristikas?
10. Ar sistema naudoja biometrinius modelius ar biometrinius atvaizdus, ar ir viena, ir kita?

Panaudojant aukščiau paminėtus klausimus, kaip pavyzdį, galime paimti ir įvertinti viešai įrengtą verifikavimo sistemą, kuri veikia su asmens kortelėje įrašytais asmens biometriniais duomenimis. Šiuo atveju grėsmė privatumui žymiai mažesnė nei slaptos identifikavimo sistemos su centralizuota duomenų baze atveju. Net jeigu minėti klausimai neapima visų galimų grėsmių, privatumui kylančios grėsmės konstatavimas gali būti priimtas tam, kad būtų įvertintas galimas bet kokios sistemos netinkamas naudojimas.

---

[43] Clarke R., Privacy Impact Assessments, Xamax Consultancy Pty Ltd, 2003. // http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html; Prisijungimo laikas: 2006-10-07.

[44] The Bioprivacy Initiative: A Framework For Evaluating The Privacy Impact Of Biometric Deployment And Technologies. International Biometric Group (IBG), M1/03-0227, 2002 // http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/14-Bio-Privacy.pdf; Prisijungimo laikas: 2007-09-12.

[45] Pavyzdžiui kortelėje.

## 3.3. Privatumo apsauga biometrijos kontekste

Baimės, atsirandančios dėl biometrinių sistemų naudojimo, yra pagrįstos, tačiau perdėtai atsargus požiūris į tai gali duoti priešingus nei galima tikėtis rezultatus. Pažymėtina, kad tie, kurie mano, kad bet koks biometrinių duomenų naudojimas riboja privatumą, taip pat tie, kurių nuomone, biometriniai duomenys turėtų būti naudojami visuose sandoriuose, užkerta kelią diskusijoms, todėl tokie požiūriai nėra tinkami.[46] Proporcingumo principas reikalauja rasti teisingą pusiausvyrą.

2005 m. Šveicarijoje 27-osios Tarptautinės duomenų apsaugos ir privatumo įgaliotinių konferencijos rezoliucijoje dėl biometrijos naudojimo pasuose, tapatybės kortelėse ir kelionės dokumentuose,[47] nurodoma, kad platus biometrijos naudojimas turės ilgalaikės įtakos pasaulio visuomenei ir todėl tai turėtų būti atviros pasaulinės diskusijos tema. Atsižvelgiant į tai, rezoliucijoje rekomenduojama (raginama):

- Įgyvendinti efektyvias apsaugos priemones ankstyvojoje stadijoje siekiant sumažinti biometrijos keliamą riziką.
- Tiksliai atskirti biometrijos duomenis renkamus ir saugomus visuomenės tikslams (pvz., pasienio kontrolei), remiantis teisinėmis prievolėmis nuo renkamų ir saugomų sutartiniams tikslams, remiantis sutikimu.
- Riboti techninį biometrijos naudojimą pasuose ir tapatybės kortelėse tikrinimo tikslais lyginant asmens dokumento duomenis su duomenimis, gautais duomenų savininkui pateikus asmens dokumentą.

P. Rosenzweig ir kiti autoriai nurodo, kad biometriniai duomenys, kaip saugumo priemonė, negali būti suabsoliutinti: „sistema negali būti laikoma vieninteliu saugumo garantu bei idealiu sprendimu; tai – tik vienas iš daugelio įrankių, naudojamų siekiant užtikrinti saugumą“. Atsižvelgiant į tai, pateikiama keletas sprendimų, galinčių padėti apsaugoti asmens privatumą naudojant biometrinius duomenis. Siekiant užtikrinti ir laisvę bei privatumą, ir sustiprinti saugumą, yra teikiamos rekomendacijos dėl šių pagrindinių principų įgyvendinimo[48]:

---

[46] Rosenzweig P., Kochems A., Schwartz A. Biometric technologies: Security, legal, and policy implications // Legal Memorandum, 12 tomas, 2004. // http://www.heritage.org/Research/HomelandSecurity/lm12.cfm; Prisijungmo laikas: 2006-09-18.

[47] Rezoliucija dėl biometrijos naudojimo pasuose, identifikavimo kortelėse bei kelionės dokumentuose, 27-oji Tarptautinė duomenų apsaugos ir privatumo įgaliotinių konferencija, Montreux, 2005 m. rugsėjo 16 d. // http://www.ada.lt/images/cms/File/rezoliucija_konferencijos_medz.pdf; Prisijungimo laikas: 2007-09-10.

[48] Rosenzweig P., Kochems A., Schwartz A. Biometric technologies: Security, legal, and policy implications // Legal Memorandum, 12 tomas, 2004. // http://www.heritage.org/Research/HomelandSecurity/lm12.cfm; Prisijungmo laikas: 2006-09-18.

- aplinka turi būti ne slapta, bet atvira;
- sistema turi naudoti ne identifikavimo, o verifikavimo/autentifikavimo funkciją;
- sistemos duomenys turi būti saugomi ne centralizuotoje duomenų bazėje, o vietiniu lygiu;
- sistema neturi būti privaloma, ji turi numatyti pasirinkimo galimybę;
- atitikimo procesas turėtų būti grindžiamas ne saugomu atvaizdu, o šablonu;
- turėtų būti garantuojamas slaptumas;
- sistema turi būti apsaugota nuo netinkamo jos naudojimo;
- turėtų būti atliekamas įprastinis antrinis patikrinimas;
- atitinkama antrinė tapatybės nustatymo sistema turėtų būti sukuriama tiems atvejams, kai pirminė sistema neveikia.

IBM specialistai pasiūlė kitą būdą privatumui biometrinėje aplinkoje apsaugoti[49]. Biometrinis ryšys turi būti pakeičiamas „esant pasikartojantiems, nepašalinamiems biometrinio ryšio iškraipymams“[50] tam, kad būtų išvengta galinčio jam kilti pavojaus. Pankanti ir kitų nuomone[51], privatumo sustiprinimui tinkamas toks sprendimas: sistema turėtų naudoti decentralizuotą atpažinimo procesą, o biometrinių duomenų asmens kortelėje naudojimas galėtų būti tinkamas sprendimas tais atvejais, kai naudojama pirštų atspaudų technologija. Taip pat reikia pažymėti, kad: patikėtos informacijos privatumą turėtų apsaugoti sistemos vykdytojai; tam tikra informacija apie sistemas ir jų naudojimą turėtų būti paskelbiama visuomenei, o technologijos turėtų būti naudojamos socialiai patikimu būdu, taip sumažinant netinkamo sistemų naudojimo galimybę.[52] Šių priemonių visuma laikoma pakankama privatumo ir saugumo apsaugai: „atsakingai ir patikimai naudojant biometrines sistemas, asmens privatumą iš tiesų galima apsaugoti.“[53]

Praktinio privatumo apsaugos modelio pavyzdžiu laikytinas vieną efektyviausių tokių sistemų įdiegusios Ontario provincijos (Kanada) Informacijos ir privatumo komisarės rekomendacijoje, skirtoje Toronto socialinės apsaugos sistemos, kurioje naudojami pirštų atspaudai, tobulinimui:

- biometriniai duomenys (šiuo atveju nuskenuotas piršto atspaudas) turi būti užkoduoti;

---

[49]Ratha N. K., Connell J. H., Bolle R. M. Enhancing security and privacy in biometrics-based authentication systems, 2001. // http://www.research.ibm.com/journal/sj/403/ratha.html; Prisijungimo laikas: 2007-10-04.
[50] Ten pat.
[51] Pankanti S., Prabhakar S., Jain A. K. Biometric recognition: Security and privacy concerns, 2003. // http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf; Prisijungimo laikas: 2007-10-27.
[52] Bowyer K. W. Face recognition technology: Security versus privacy. IEEE Technology and Society Magazine. Nr. 1(23), 2003). P. 9 // http://www.cse.nd.edu/Reports/2004/TR-2004-21.pdf; Prisijungimo laikas: 2007-10-23.
[53] Pankanti S., Prabhakar S., Jain A. K. Biometric recognition: Security and privacy concerns, 2003. // http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf; Prisijungimo laikas: 2007-10-27.

- užkoduotas piršto atspaudo atvaizdas gali būti naudojamas tik paliudyti tinkamumui, užtikrinant, kad jis nebus naudojamas kaip socialinės kontrolės ar sekimo priemonė;
- privaloma užtikrinti, kad identifikuojamas piršto atspaudas negalėtų būti atkurtas iš užkoduoto piršto atspaudo atvaizdo, saugomo duomenų bazėje;
- privaloma užtikrinti, kad nežinomas piršto atspaudas (pvz. paimtas nusikaltimo vietoje) negalėtų būti sutapatintas su užkoduotu piršto atspaudo atvaizdu, saugomu duomenų bazėje;
- privaloma užtikrinti, kad užkoduotas piršto atspaudo atvaizdas negalėtų būti naudojamas kaip vienintelis identifikatorius;
- privaloma užtikrinti, kad užkoduotas piršto atspaudo atvaizdas nebūtų naudojamas identifikuoti asmenį (t.y. tokiu būdu, kokiu gali būti naudojamas pats piršto atspaudas);
- privaloma užtikrinti griežtą teisės prieiti prie biometrinės informacijos kontrolę ir tokios prieigos pagrįstumą;
- tam, kad duomenimis galėtų pasinaudoti valstybinės institucijos, pvz., policija, ar kitos teisėsaugos institucijos, būtinas įgaliojimas ar teismo sprendimas;
- privaloma užtikrinti, kad duomenys apie bet kokios naudos gavimą (t.y. asmeninė informacija apie, pvz., atliktų mokėjimų istoriją ir t.t.) būtų saugomi atskirai nuo asmenį identifikuojančių duomenų – vardo, gimimo datos ir t.t.; [54]

Apibendrinant, pažymėtina, jog tiek tarptautinių susitarimų, tiek biometrijos pramonės įmonių, tiek ir atskirų valstybių siūlomuose ir diegiamuose biometrijos naudojimą reglamentuojančiuose dokumentuose akcentuojama valstybės valdymo institucijų pareiga biometrinių sistemų ir biometrinių tapatybės dokumentų srityje diegti teisines ir technines apsaugos priemones tiek pačiuose dokumentuose, tieks ir biometrinėse atpažinimo sistemose. Taip pat akcentuojamas poreikis užtikrinti, kad biometriniai duomenys būtų renkami ir naudojami pagrįstais tikslais, tiek numatytais įstatymuose, tiek ir susitarimų su duomenų savininku pagrindu, naudojamus duomenis maksimaliai apsaugant nuo neautorizuotos prieigos. Dar vienas esminis principas – atsargus biometrijos vertinimas, siekiant užtikrinti, kad ja paremtos sistemos nebūtų laikomos idealiu saugumo problemų sprendimu, o jų technologiniai trūkumai nebūtų mėginami kompensuoti papildomų biometrinių duomenų naudojimu ir visaapimančių biometrinių sistemų kūrimu, vietoje to numatant ir alternatyvios patikros įprastinėmis priemonėmis galimybes. Kiekvienoje valstybėje asmens duomenų rinkimo bei priėjimo prie jų kontrolės funkciją siūloma

[54] Cavoukian A. Privacy and biometrics: An oxymoron or time to take a 2nd look?, 1998. // http://www.ipc.on.ca/index.asp?layid=86&fid1=98; Prisijungimo laikas: 2006-10-07.

pavesti nepriklausomai institucijai, pavyzdžiui tokiai kaip Prancūzijos Nacionalinė informatikos ir laisvių komisija[55], nuolat kontroliuoti.

### *4. Biometrinių duomenų apdorojimo sąlygojamos grėsmės*

Pradėjus masiškai naudoti biometrines technologijas, iškilo poreikis teisiškai išanalizuoti, ar šie nauji būdai neprieštarauja teisės principams bei egzistuojančiai teisinei bazei. Biometrinių technologijų naudojimas pagrindiniuose asmens identifikavimo dokumentuose sąlygoja dvejų pagrindinių tipų grėsmes: susijusias su galimais teisės į privatų gyvenimą pažeidimais bei susijusius su šių duomenų ir taikomų technologijų patikimumo klausimu.

Pirmojo tipo grėsmės, sąlygojamos biometrinių duomenų specifikos bei saugojimo būdų, yra susijusios su neautorizuoto saugomų biometrinių duomenų panaudojimo galimybe. Dėl ypatingos biometrinių duomenų prigimties, kai kurie jų turi labai daug informacijos, pagal kurią galima ne tik identifikuoti asmenį, bet ir pvz. piršto atspaudų duomenys gali nurodyti įvairias genetines anomalijas, ar polinkį į tam tikras ligas.[56] Be to, kai kurios biometriniam atpažinimui naudojamos technologijos (piršto antspaudas, kurį galima ir vėliau nuimti nuo asmens liesto daikto, nuotolinis video atpažinimas) sudaro sąlygas jas naudoti be asmens sutikimo. Net ir neapdorotų biometrinių duomenų kaupimas sąlygoja grėsmes dėl galimybės juose aptikti svarbios papildomos informacijos, ypač apie sveikatą. Kovai su pastarąja grėsme jau 1981 m. buvo skirta pirmoji Europos ekonominės bendrijos (EEB) Ministrų Tarybos rekomendacija duomenų apsaugos srityje.[57] Nors naudojant koduotą informaciją bei ją laikant tik mediciniškai reikalingą laiko tarpą tikėtina, jog šios grėsmės sumažės, tačiau literatūroje vyrauja nuomonė, kad šis teiginys būtų patvirtintas, reikia atlikti daugiau tyrimų šiam aspektui ištirti.

Antroji, duomenų patikimumo problema, yra labiau techninio pobūdžio ir susijusi su biometrijoje naudojamos techninės įrangos pajėgumu atpažinti konkrečius identifikuojamo asmens požymius.

---

[55] Prancūzijos duomenų apsaugos institucija yra žinoma, kaip Commission nationale de l'informatique et des libertés (CNIL). Reikia pažymėti, kad CNIL didelį autoritetą duomenų apsaugos srityje turinti institucija.
[56] Hopkins J. Gastroenterology: Fingerprinting GI Disease.// Physician Update.. April 1996. P. 5.
[57] Ministrų komiteto Rekomendacija Nr. R (81) 1 valstybėms narėms dėl automatizuotų medicininių duomenų bankų nuostatų, priimta Ministrų komiteto 1981 m. sausio 23 d. 328-ame viceministrų lygio susitikime), http://www.ada.lt/images/cms/File/Rekomendacija%20Nr.%20R%20(81)%201.pdf; Prisijungimo laikas: 2007-10-29.

## 4.1. Biometrinių duomenų naudojimas: autentifikavimas vs identifikavimas

Biometrinių technologijų naudojimas reiškia, jog unikalūs asmens biologiniai ir/arba elgesio požymiai yra surenkami ir saugomi tam, kad būtų galima autentifikuoti (patikrinti tapatybę) arba identifikuoti (nustatyti tapatybę). Šiame apibrėžime minimos dvi pagrindinės biometrinių sistemų funkcijos, kurios labai skiriasi ne tik savo tikslais, bet taip pat būdu, kuriuo yra vykdomos: (1) autentifikavimas funkcija, kuri reiškia palyginimą vienas prieš vieną (1:1) ir kuri leidžia patikrinti asmens reikalavimo pagrįstumą (pavyzdžiui, „Aš turiu darbuotojo kortelę, kuri buvo išduota man, ir turiu teisę įeiti į šias patalpas“) ir (2) identifikavimo funkcija, kuri yra vieno palyginimas su daugeliu (1:N) ir kuri leidžia nustatyti, ar biometriniai požymiai yra centrinėje duomenų bazėje (tam, kad būtų išvengta „dvigubos naudos gavimo“, pvz., prieglobsčio prašančiojo atveju, kai jis jau dėl to kreipėsi kitoje valstybėje), arba, jeigu vardai yra įtraukti į šią duomenų bazę, nustatyti, kam konkretus biometrinis požymis priklauso.

Nagrinėjant galimas grėsmes, svarbu atskirti šias dvi biometrinių duomenų funkcijas. Autentifikavimo funkcija dažniausiai yra naudojama padaryti tapatybės patikrinimo procesą saugesnį, prie to, kas „esate“, pridedant tai, ką „turite“ ir ką „žinote“. Autentifikavimo funkcija taip pat sudaro galimybę biometrinius požymius saugoti vietiniu lygiu, kontroliuojant asmeniui (pvz. kortelėje). Grėsmė, kad biometriniai duomenys bus panaudoti to asmens identifikavimui arba kad bus panaudoti kitu tikslu („funkcijos deformacija“, t.y. grėsmė, kad duomenys bus panaudoti šalutiniams tikslams, nesuderinamiems su tikslais, kuriems duomenys iš pat pradžių buvo renkami), išlieka ribota, palyginus su biometrinių požymių naudojimu atliekant identifikavimo funkciją, su sąlyga, kad biometrinė sistema yra įgyvendinta tinkamai. Pažymėtina, kad biometrinių duomenų identifikavimo funkcija kelia daugiausia problemų ir sąlygoja daugelį grėsmių (tokių kaip sekimas arba tapatybės pasisavinimas), kadangi biometriniai duomenys daugiau nebėra kontroliuojami (fiziškai) to asmens, kuriam jie priklauso. Šios problemos tapo dar realesnės, kai kurioms valstybėms pradėjus kurti didelio masto pasų ir elektroninių tapatybės kortelių su privalomais biometriniais požymiais centralizuotas duomenų bazes (pvz. Jungtinė Karalystė). Šios duomenų bazės su piliečių, kurių kiekvieno bus susietas su biometriniais požymiais, vardais ir adresais (o dažnai ir su kita informacija), leis valdžiai, o taip pat ir privatiems asmenims, kurie turi teisę prieiti prie duomenų, identifikuoti asmenis tiesiog pateikiant vieną iš registruotų biometrinių požymių.

## 4.2. 29 straipsnio Darbo grupės išvada dėl biometrinių duomenų

Kaip jau buvo minėta darbo įvade, atsižvelgiant į didelę Europos Sąjungos svarbą biometrijos technologijų naudojimo ir reglamentavimo srityje, šiame darbe atliekama biometrinių duomenų privatumo ir apsaugos problemų analizė orientuosis į Europos S1jungos 29 straipsnio Darbo grupės asmenų apsaugai tvarkant asmens duomenis 2003 m. rugpjūčio 1 d. išvadose iškeltus klausimus. Šie klausimai išlieka svarbūs kaip atspirties taškas tolesnėms diskusijoms apie biometrinių duomenų teisinius aspektus. Šioje darbo dalyje pagrindinis dėmesys bus skiriamas dvejoms išvados dalims.

Darbo grupės išvada pirmiausia skirta biometrinių duomenų naudojimui patikrinimo tikslais. Kodėl Darbo grupė koncentruojasi ties patikrinimu, aiškintina tuo faktu, kad 2003 m. biometrinės technologijos, skirtos identifikavimui, dar nebuvo iki galo išsivysčiusios. Darbo grupė remiasi duomenų bazės dydžiu ir biometriniais duomenimis, kaip faktoriais, kurie tuo metu buvo lemiami idant būtų įmanoma atlikti identifikavimo funkciją. Tuo tarpu vystantis technologijoms bei tobulėjant identifikavimo pagal biometrinius duomenis galimybėms kai kuriose šalyse buvo įkurti centriniai nacionaliniai registrai su centrinėmis duomenų bazėmis, apimančiomis ir identifikavimui skirtus biometrinius požymius.[58]

Diskusijoje apie tikslingumo ir proporcingumo principų taikymą Darbo grupė aptaria pavyzdį, kai biometriniai duomenys naudojami kontrolės tikslais ir tokiu būdu remiasi patikrinimo funkcija. Kita vertus, savo išvadoje Darbo grupė bendrai apibūdina biometriniams duomenims galinčias kilti grėsmes, nesvarbu, ar duomenys naudojami identifikavimo, ar autentifikavimo tikslais, pvz., slaptą informaciją apimančius biometrinius duomenis, slaptą rinkimą, klaidingo atmetimo laipsnį (angl. *false reject rate* - FRR), taip pat klaidingo priėmimo laipsnį (angl. – *false accept rate* – FAR), ir vagystę, kas kelia grėsmę tiek patikrinimui, tiek identifikavimui naudojamiems duomenims. Kitos apibūdintos grėsmės, kaip, pvz., sekimas, netinkamas pakartotinis duomenų panaudojimas, kaip unikalaus identifikatoriaus naudojimas ir identifikavimas yra grėsmės, kurios iš tikrųjų gali atsirasti tik biometrinius duomenis naudojant centralizuotu būdu.

Darbo Grupės pozicija dėl to, ar biometriniai duomenys turi būti naudojami tik autentifikacijai, nėra pilnai ta ir lieka neaiški. Patikslinta Darbo grupės išvada dar turėjo prisidėti prie to, kad teisės aktai, reguliuojantys duomenų apsaugą biometrinėse sistemose, būtų taikomi

[58] Pavyzdžiui, Jungtinė Karalystė, kur Nacionalinis tapatybės registras, kuris bus įsteigtas pagal 2006 m. Tapatybės kortelių aktą, ir kurio centrinėje duomenų bazėje bus kaupiami biometriniai duomenys. Apie tai bus rašoma šio magistrinio darbo dalyje apie biometrinius pasus

efektyviai ir vienodai. Kadangi išvada, kaip gairėmis tolesniam duomenų apsaugos teisės aktų interpretavimui, naudojasi nacionalinės duomenų apsaugos institucijos, toks patikslinimas yra reikalingas Darbo Grupės sau keliamų tikslų prasme.

Pažymėtina, kad būtina atkreipti dėmesį ir į kitą išvados dalį, t.y. į tikslo ir proporcingumo principo taikymą. Darbo grupė savo išvadoje konstatavo, kad tikslo ir proporcingumo principas teisinėse duomenų apsaugos institucijų biometrinių sistemų apžvalgose turi būti lemiamas faktorius. Tačiau egzistuoja tam tikras teisinis neaiškumas, t.y. neaišku, kaip tikslo ir proporcingumo principas turi būti taikomas apdorojant asmens duomenis apskritai ir ypač – biometrinius duomenis. Šis klausimas bus nagrinėjamas aptariant Asmens duomenų apsaugos direktyvos taikymą biometrijoje.

## 4.3. Kiti biometrinių duomenų naudojimo aspektai

Aukščiau aptartos 29 straipsnio Darbo grupės išvados buvo parengtos sparčios biometrinių technologijų plėtros kontekste. Atsižvelgdama į sparčią biometrinių technologijų raidą, Darbo grupė nurodė, kad jos išvada yra tik „darbinis dokumentas“, kurį ji ketina peržiūrėti, atsižvelgdama „į duomenų apsaugos institucijų patirtį ir technologijų plėtrą, susijusią su biometrinių duomenų taikymą“[59]. Nors šis dokumentas kol kas nėra atnaujintas, šiuo metu galima išskirti keletą pagrindinių problemų, nepakankamai 2003 m. pateiktose Išvadose: tai yra galimybė duomenis valdyti privačiam subjektui, duomenų kokybės ir laikmenų patikimumo užtikrinimo klausimas, galimybė neteisėtai naudoti duomenis.

Biometrinių technologijų plėtra kelia pagrįstą klausimą dėl to, kas gali būti jų tvarkytoju: ar tik valstybinės institucijos, ar tokia teisė gali būti deleguojama ir privatiems subjektams, jei taip, tai kokia apimtimi šios privačios organizacijos turi turėti teisę kontroliuoti asmenų tapatybę. Bet koks atsakymas į šį klausimą gali sukelti įvairių politinių interpretacijų – nuo kaltinimų valstybei siekiu monopolizuoti viso piliečių gyvenimo kontrolę (biometrinio „didžiojo brolio“ atsiradimo scenarijus‘)[60] iki įtarimų, jog privatūs subjektai įgis galimybes slapta rinkti asmeninius duomenis.

Teisiniu aspektu šis klausimas iš dalies yra išspręstas direktyva 95/46/EB, nustatant, kad duomenis gali valdyti tiek viešas, tiek ir privatus valdytojas. Tačiau tuo atveju, jei biometrinius duomenis įėjimo (patekimo) kontrolės tikslais naudoja privatus valdytojas, pvz., į atvirą visuomenei

[59] Direktyvos 95/46/EB 29 str. darbo grupės 2001 m. rugsėjo 13 d. Darbinis dokumentas Nr. 12168/02, WP 80 „Dėl biometrinių duomenų“// http://www.ada.lt/images/cms/File/WP80.pdf; Prisijungimo laikas: 2007-08-29.
[60] Woodward J. D. Biometrics: Privacy’s foe or privacy’s friend? // Proceedings of the IEEE, Nr. 9, 1997. // http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf Prisijungimo laikas: 2007-11-07. P. 11.

vietą – futbolo stadioną, vadovaujamasi viešuoju interesu (tvarkos (viešosios) užtikrinimu), arba kontroliuojančio asmens interesai nusveria asmeninius interesus[61]. Direktyva 95/46/EB nustato, kad jeigu duomenų apdorojimas remiasi tokiais principais, duomenų subjektai privalėtų turėti teisę „remdamiesi privalomu teisėtu pagrindu, susijusiu su jo konkrečia situacija, bet kuriuo metu prieštarauti“ duomenų apie jį tvarkymui, nebent nacionaliniai įstatymai nustato ką kita[62]. Teisėtu pagrindu gali būti požiūris, kad biometriniai duomenys apima neskelbtiną informaciją, registravimosi sunkumai, arba religiniai įsitikinimai. Principas, kuris leidžia asmenims prieštarauti dėl jų duomenų tvarkymo, yra aktualus diskutuojant apie biometrinius duomenis. Todėl į biometrines sistemas greičiausiai niekada nebus įtraukti duomenys apie absoliučiai visus asmenis, kuriems tos sistemos skirtos (pvz., keleivių patekimo į tam tikras oro uostų zonas kontrolė).

Vienas pagrindinių duomenų apsaugos principų, įtvirtintų Direktyvoje 95/46/EB, yra duomenų kokybė. Šis principas reiškia, kad asmeniniai duomenys turi būti „*tikslūs* ir, jei būtina, *nuolat atnaujinami*“. Be to, „turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginti su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų *ištrinti arba ištaisyti*“[63].

Šis duomenų kokybės reikalavimas kelia problemų specifinių biometrinių duomenų atveju, t.y. duomenų, susijusių su žmogaus savybėmis, kurios keičiasi laikui bėgant, pvz., asmeniui senstant. Biometriniai duomenys, susiję su jaunesnių asmenų rankų geometrija ar veidu, pavyzdžiui, vaikų, gali tam tikru metu nebebūti „tinkamos kokybės“, kadangi jų savybės keičiasi, ir šie pokyčiai nėra atspindėti duomenyse. Ši problema buvo pripažinta 2005 m. Nyderlandų Vidaus reikalų ministerijos atliktame tyrime, analizuojant vaikų veido atvaizdo naudojimą tapatybės dokumentams. Tyrimo ataskaitoje buvo konstatuota, kad “labai tikėtina, jog dvylikos metų ar jaunesnių vaikų veido atpažinimas iš keleto metų senumo atvaizdo, yra problematiškas. To priežastis yra žymūs veido bruožų proporcijų pokyčiai, vykstantys augant. Šie pokyčiai yra sudėtingas procesas, kuris yra labiausiai nulemtas lyties ir genetinių faktorių“[64]. Be to, ataskaitoje teigiama, kad egzistuoja problema ir tais atvejais, kai vaikai yra vyresni nei dvylikos metų, ir kad šiuo klausimu tikslinga atlikti papildomus tyrimus. Todėl duomenų kokybė, kalbant apie biometrinius jaunų asmenų

---

[61] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15., 7(e) ir (f) straipsniai 7(e) ir (f) straipsniai.

[62] Ten pat14 (a) straipsnis.

[63] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15., 6. 1 (d) straipsnis.

[64] Ministry of the Interior and Kingdom Relations. Evaluation ReportBiometrics Trial: 2b or not 2b. 2005 // www.minbzk.nl/contents/pages/48403/trailreportbiometrics.doc.pdf ; Prisijungimo laikas: 2007-10-03.

duomenis, yra ne tik praktinė problema, bet ir teisinės bazės duomenų apsaugos srityje požiūriu, kadangi joje įtvirtinti duomenų kokybės reikalavimai, t.y., kad duomenys turi būti tikslūs. Netikslūs duomenys sąlygotų klaidingo atmetimo/klaidingo priėmimo laipsnio padidėjimą ir paverstų visą biometrinių duomenų programą nepatikima. Klaidingo atmetimo/klaidingo priėmimo laipsnis taip pat kelia grėsmę duomenų subjektams, nes vietoje subjekto gali būti identifikuotas kažkas kitas arba jo prašymui gali būti nepagrįstai atsakyta. Ši problema yra ypač aktuali, kadangi biometrinės programos patogumo ar kitais sumetimais dažnai naudojamos mokyklose ar kitur, kur vaikai sudaro didžiąją dalį (pavyzdžiui, paskirstant maistą)[65].

Kaip minėta aukščiau, asmeniniams duomenims keliami tikslumo reikalavimai. Esminė biometrinių sistemų savybė yra derantis sprendimas. Dėl būdingos statistinės biometrinių sistemų prigimties, biometrinės sistemos sprendimas reiškia tik santykį tarp pateiktų biometrinių pavyzdžių ir nurodytų duomenų. Kiekvienas biometrinių sistemų tipas turi aukštesnio ar žemesnio laipsnio klaidingo atmetimo ir klaidingo priėmimo tikimybes. Sistemos operatorius arba projektuotojas privalo nustatyti priimtinas ribas ir priimtiną klaidų laipsnį; dėl to sprendimas paprastai priimamas atsižvelgiant į konkrečios programos reikalavimus. Programose, turinčiose žemą saugumo laipsnį, pvz., moksleivių maisto registravimo sistemoje, gali būti nuspręsta sumažinti klaidingo atmetimo galimybę, o tai savaime sąlygos klaidingo priėmimo laipsnio išaugimą. Toks sukeitimas ir faktas, kad atitikimas niekada nėra absoliutus, o tik galimybė, reiškia, jog sprendimai, kuriuos biometrinė sistema priima asmens atžvilgiu, ir su juo susiję duomenys, niekada nėra 100 % teisingi.

Lietuvos žmogaus teisių stebėjimo instituto direktorius H.Mickevičiaus teigimu, remiantis Didžiojoje Britanijoje 2005 m. paskelbtais tyrimų duomenimis, identifikavimo sistemos pagal veido biometrinius duomenis tiksliai atpažino 69% sveikų žmonių ir tik 48% asmenų su negalia. Pirštų atspaudų atpažinimas buvo tikslus 80% atvejų. Panašūs rezultatai buvo gauti ir atlikus bandymus Vokietijoje bei JAV.[66]

Dar vienas su biometrinių technologijų naudojimu susijęs neaiškumas yra jų patikimumas laike. Kaip jau buvo minėta darbo įvade, nors biometrinės technologijos eksperimentiniais tikslais naudojamos tik nuo aštuntojo-devintojo dešimtmečio, tačiau nėra ilgalaikės masinės jų kasdienio naudojimo patirties. Dėl šių priežasčių apie biometrijai naudojamų laikmenų patikimumą galima spręsti tik remiantis teorinių ir laboratorinių bandymų rezultatais.

---

[65] Wendy M. Grossman. Is school fingerprinting out of bounds?, 2003 // http://www.guardian.co.uk/technology/2006/mar/30/schools.guardianweeklytechnologysection; Prisijungimo laikas: 2007-11-07.

[66] Mickevičius H. Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą, Žmogaus teisių stebėjimo institutas, 2006. // http://www.hrmi.lt/news.php?strid=1999&id=3455; Prisijungimo laikas: 2007-08-29.

Labai svarbus su biometrinių duomenų saugumu susijęs klausimas yra galimybė suklaidinti biometrines sistemas neteisėtai pasisavintais duomenimis. Šiuo atveju, nors sukauptų duomenų saugumas nėra tiesiogiai susijęs su biometrija, o yra labiau techninis informatikos klausimas, tačiau jo svarbą ir teisniu apsektu suponuoja faktas, jog įgavus prieigą suteikiančius duomenis vien tik biometrija paremtos technologijos tampa bejėgės.

Šios techninės charakteristikos kelia klausimą ar galima laikyti, jog biometrinės sistemos atitinka direktyvos reikalavimus dėl asmens duomenų tikslumo?

Kaip matyti iš aptartų techninių aspektų, biometrinės sistemos gali neatitikti šio kriterijaus, todėl visada lieka tikimybė, jog bus priimami neteisingi sprendimai. Be to, ir pati IBG pažymi, jog „biometrijoje tobulybė neegzistuoja“.[67] Šiam požiūriui pritaria ir P.Rosenzweig teigdamas, kad biometriniai duomenys, kaip saugumo priemonė, negali būti suabsoliutinti: „sistema negali būti laikoma vieninteliu saugumo garantu bei idealiu sprendimu; tai – tik vienas iš daugelio įrankių, naudojamų siekiant užtikrinti saugumą“[68]: Kaip matyti iš aptartos biometrijos naudojimo problematikos, ši technologija turi ženklių trūkumų, susijusių tiek su jos gebėjimu atpažinti asmenis, tiek ir galimybe piktnaudžiauti neteisėtai įgytais duomenimis. Atsižvelgiant į aptartą problematiką bei išsivystymo lygį, biometrijos technologijų naudojimas turėtų būti ribojamas, numatant duomenų taisymo galimybes bei, labiau saugumo ir tikslumo reikalaujančiais atvejais – ir papildomas kontrolės priemones.

[67] Guerrier C., Cornelie, L-A., Les aspects juridiques de la biometrie. P. 2. // http://www.biometrie-online.net/dossiers/generalites/droit/Claudine%20GUERRIER.pdf; Prisijungimo laikas: 207-09-23.
[68] Rosenzweig, P., Kochems, A.and Schwartz, A., Biometric technologies: Security, legal, and policy implications. Legal Memorandum, 12 tomas. 2004. // http://www.heritage.org/Research/HomelandSecurity/lm12.cfm; Prisijungmo laikas: 2006-09-18.

# II. Tarptautinės pastangos užtikrinti asmens duomenų apsaugą biometrijos kontekste

Šioje darbo dalyje aptariamas biometrijos technologijų poveikis asmens duomenų apsaugai, aptariant jį kelias aspektais. Pirmiausia analizuojami tarptautiniu ir Europos Sąjungos mastu priimti teisės aktai, reguliuojantys asmens duomenų apsaugą biometrijos kontekste. Kitas svarbus aspektas – tai Direktyvos 95/46/EB „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“ taikymas biometriniams duomenims. Taip pat bus aptariama Direktyvos taikymas ES valstybėse narėse ir tikslingumo ir proporcingumo principų taikymas.

## *1. Ekonominio bendradarbiavimo ir plėtros organizacijos veikla*

Vienu pirmųjų mėginimų tarptautiniu lygmeniu reglamentuoti asmens duomenų apsaugą naudojant informacines technologijas sietinas su 1980 m. priimta labiausiai išsivysčiusias pasaulio valstybes vienijančios Ekonominio bendradarbiavimo ir plėtros organizacijos Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių (toliau – Gairės)[69]. Šis dokumentas laikytinas fundamentaliu aktu, tarptautiniu lygmeniu pirmą kartą susisteminančiu ir įtvirtinančiu esminius asmens duomenų tvarkymo principus. Gairės taikomos bet kokiai „informacijai, susijusiai su identifikuotu ar identifikuotinu asmeniu (duomenų subjektu)“[70], tai yra kurio tapatybė yra nustatyta ar gali būti nustatyta. Jos taikomos tiek privačiajam, tiek ir viešajam sektoriui, visoms kompiuterizuoto asmens duomenų tvarkymo sistemoms ir priemonėms[71] ir apima bet kokį asmens duomenų tvarkymą ar naudojimą.

Gairės įtvirtina 8 esminius asmens duomenų tvarkymo principus:

**Asmens duomenų rinkimo apribojimo principas** pabrėžia būtinybę, kad būtų nustatytos asmens duomenų rinkimo apimties ribos, o bet kokie asmens duomenys būtų gaunami teisėtai ir naudojant teisėtas priemones, apie tai žinant pačiam asmens duomenų subjektui ir esant jo sutikimui.

[69] 1980 m. rugsėjo 23 d. EBPO Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių. // http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html; Prisijungimo laikas: 2007-11-10

[70] Ten pat, 1 skirsnis.

[71] Ten pat, 2 ir 3 skirsniai

**Asmens duomenų kokybės principas** - asmens duomenys turi atitikti tikslus, kuriems jie yra ar bus naudojami. Be to, duomenys turi būti kiek įmanoma tikslūs ir nuolat atnaujinami.

**Tikslo nustatymo principas** išreiškia būtinybę ne vėliau nei asmens duomenų rinkimo metu nurodyti tikslus, kuriems renkami asmens duomenys. Tolesnis duomenų naudojimas yra apribojamas tais pačiais tikslais arba kitais, kurie nėra nurodyti, bet yra suderinami su anksčiau nurodytais.

**Asmens duomenų naudojimo apribojimo principas** - asmens duomenys negali būti atskleisti ar tapti prieinami dėl kitų priežasčių, išskyrus tuos atvejus, kai gaunamas asmens duomenų subjekto sutikimas arba kai taip nurodyta įstatyme.

**Saugumo užtikrinimo principas** - asmens duomenys privalo būti protingomis priemonėmis apsaugoti nuo tokių pavojų kaip asmens duomenų netekimas, praradimas, neteisėtas priėjimas prie asmens duomenų, jų sunaikinimas, panaudojimas, pakeitimas ar atskleidimas.

**Atvirumo principas** - turi būti nustatyta bendra atvirumo politika dėl asmens duomenų vystymosi, formavimosi, praktikos ir pan. Priemonės turi būti prieinamos ir tinkamos, siekiant nustatyti asmens duomenų buvimą ir prigimtį, jų naudojimo pagrindinį tikslą, taipogi asmens duomenų valdytojo tapatybę ir jo buvimo vietą.

**Individualaus dalyvavimo principas** reiškia asmens teisę:

- kad suprantamu būdu, per protingą laiko tarpą ir už ne per didelį mokestį jam būtų pranešta apie duomenis, kuriuos asmens duomenų valdytojas turi apie jį;
- jei atsisakoma pranešti kokius duomenis apie renka asmens duomenų valdytojas, turi būti nurodomos priežastys ir motyvai, suteikiant teisę ginčyti tokius nesuteikimo pagrindus;
- ginčyti jo manymu neteisingus asmens duomenis, reikalauti jų pataisymo, papildymo, pakeitimo ar panaikinimo.

**Atskaitomybės principas –** asmens duomenų valdytojas privalo būti atskaitingas už tai, kaip jis laikosi priemonių, kurios įgyvendina anksčiau nurodytus principus.

Reikia paminėti, kad nors „EBPO Tarybos rekomendacijos nėra teisiškai privalomos ir greičiau išreiškia politinę, moralinę valstybių narių valią ir įsipareigojimus“[72], tačiau dėl politinės organizacijos svarbos bei dėl to, jog šis dokumentas buvo taikomas pagrindinių informacinių technologijų kuriančių valstybių praktikoje, jis padarė didelę įtaka viso pasaulio valstybių įstatymų leidybai. „Gairės yra visuotinai pripažintos kaip tarptautiniu lygmeniu priimtinas ir technologiniu

[72] Inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD privacy guidelines on global networks, 1999, Paris. // http://www.olis.oecd.org/olis/1998doc.nsf/8d00615172fd2a63c125685d005300b5/23ec07d41a61a5e380256810004dfeab/%24FILE/05E95540.ENG; Prisijungimo laikas: 2007-11-15.

atžvilgiu neutralus privatumo apsaugos principų rinkinys“[73], kuris išlaikė kelių dešimtmečių išbandymą. Nors šiame dokumente biometrinės technologijos nėra minimos, tačiau jame pateikiami principai taikomi visoms informacinėms technologijoms.

Pirmuoju esminiu rėminiu EBPO dokumentu, reglamentuojančiu biometrijos problematiką tapo 2004 m. paskelbta EPBO Mokslinių technologijų ir pramonės direktorato Informatikos, kompiuterių ir komunikacijos politikos komiteto Ataskaita apie biometrija paremtas technologijas (toliau – Ataskaita)[74], kurioje privatumo ir saugumo požiūriu aptariama šių technologijų nauda ir trūkumai ir bei aptariamos praktikoje jau naudojamos technologijos.

EBPO Ataskaitoje aptariamos privatumui kylančias grėsmes, kurios gali atsirasti taikant biometrinio atpažinimo technologijas. Šios grėsmės susijusios su:

1. galimu „funkcijų deformavimu“;
2. galimu biometrinių technologijų virsmu iš atpažinimo į sekimo sistemas;
3. situacijomis, kai asmens sutikimas ir žinojimas (apie duomenų rinkimą) gali būti neprivalomi, kai yra panaudojamos biometrinės technologijos.[75]

Saugumo požiūriu dokumente buvo pripažinta, kad saugumo veiksniai pirmiausiai susiję su duomenų klastojimo problemomis, kurias reikia spręsti pasitelkiant tiek technines (t.y. tobulinat sistemas), tiek ir teisines priemones.

EBPO ataskaitoje yra pateikiamos rekomendacijos, reikalingos užtikrinant biometrinių sistemų atitiktį privatumo ir saugos reikalavimams. EPBO ataskaitoje rekomenduojama:

1. Saugumą ir privatumą stiprinti priimant įstatymus ir vykdant atitinkamą vyriausybės politiką;
2. Naudoti nuo suklastojimo apsaugotą techninę įrangą;[76]
3. Naudoti „privatumą užtikrinančias apsaugos technologijas“[77], pvz. tai galėtų būti biometrinis kodavimas;
4. Sukurti technologinę apsaugos architektūrą, apimančią autentifikavimą, prieigos

[73] Inventory of instruments and mechanisms contributing to the implementation and enforcement of the OECD privacy guidelines on global networks, 1999, Paris. // http://www.olis.oecd.org/olis/1998doc.nsf/8d00615172fd2a63c125685d005300b5/23ec07d41a61a5e380256810004dfeab/%24FILE/05E95540.ENG; Prisijungimo laikas: 2007-11-15.

[74] Biometric-Based Technologies, OECD, Directorate for science, technology and industry, Committee for information, computer and communications, 30-Jun-2004, DSTI/ICCP/REG(2003)2/FINAL // http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF; Prisijungimo laikas: 2007-09-10.

[75] Biometrinių sistemų pagalba, galima slaptai rinkti ir analizuoti asmenų duomenis. Pvz. „Human ID at a Distance“ projektas, kai slaptai biometrinių sistemų pagalba yra ieškoma teroristų.

[76] Biometric-Based Technologies, Organisation for Economic Co-operation and Development, Directorate for science, technology and industry, Committee for information, computer and communications, 30-Jun-2004, DSTI/ICCP/REG(2003)2/FINAL // http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF; Prisijungimo laikas: 2007-09-10.

[77] angl. *security technology enabling privacy* – sutrumpintai jos dar vadinamos STEPs.

kontrolę, duomenų konfidencialumą, duomenų vientisumą;

5. Naudoti privatumo architektūrą (t.y., projektavimo procesą, numatantį įvairias sistemos projektavimo parinktis ir galimybę pasirinkti variantą, darantį mažiausią poveikį privatumui).[78] Naudojant tokį sistemos projektavimo metodą, galima ženkliai sumažinti nederamo informacijos atskleidimo riziką sąlygojančių klaidų galimybę.

EPBO ataskaitoje taip pat pateikiamos rekomendacijos biometrinių sistemų projektuotojams ir konstruktoriams dėl konkrečios sistemos atitikties privatumo ir saugos reikalavimams:[79]

- Atvirai ir sąžiningai informuoti apie planuojamą sistemos kūrimą;
- Užtikrinti deramą su biometrinėmis sistemomis sąveikaujančių asmenų priežiūrą;
- Numatyti tinkamus rezervinius esamų apdorojimo procedūrų variantus ir išimtis;
- Užtikrinti, kad susijusios funkcijos (pavyzdžiui, registravimas ir programos tinkamumas) remtų ir stiprintų biometrinių sistemų saugą bei privatumą ir užkirstų kelią piktnaudžiavimams, pavyzdžiui, tapatybės vagystei naudojant biometrinius duomenis;
- Prieš kuriant stambias ir ypač didelės aprėpties sistemas iš pradžių sukurti smulkias ir vidutines. Tokiu būdu, atsižvelgiant į projektavimo ir kūrimo metu įgytą patirtį, bus galima efektyviau spręsti kylančias problemas, pritaikyti naujas technologijas bei atlikti patobulinimus;
- Prieš diegiant stambaus masto sistemą apsvarstyti bandomųjų sistemų ir konstrukcijų, leidžiančias biometriškai naudoti duomenis, surenkamus realiose situacijose, naudojimo galimybes;
- iki minimumo sumažinti poveikį privatumui ir padidinti biometrinį tikslumą, sutelkiant dėmesį į 1:1 autentifikavimo sistemas, o ne į 1:N identifikavimo sistemas;
- Prieš diegiant biometrines technologijas įsitikinti, kad tinkamiausias problemos sprendimas yra būtent biometrinė technologija, o ne standartinis autentifikavimo metodas. Užtikrinti, kad būtų paisoma naudotojo sutikimo ir gerbiami jo kultūriniai įsitikinimai;
- Jeigu įmanoma, sukurti sutikimu pagrįstas savanoriškos registracijos sistemas;
- Rinkti biometrinių duomenų pavyzdžius atvirai ir tik gavus naudotojo sutikimą;
- Jeigu įmanoma, suteikti naudotojui galimybę pačiam saugoti biometrinį modelį (intelektualiojoje kortelėje) ir *nelaikyti* biometrinio šablono centrinėje sistemoje.

EPBO A taskaitoje daroma išvada, kad „ateina biometrinių technologijų laikas.“[80]

[78] Ten pat. P. 39-42
[79] Ten pat. P. 37-38
[80] Biometric-Based Technologies, Organisation for Economic Co-operation and Development, Directorate for science, technology and industry, Committee for information, computer and communications, 30-Jun-2004, DSTI/ICCP/REG(2003)2/FINAL //

Atsižvelgiant į tai prognozuojama, kad mums nereikės rinktis tarp saugumo ir privatumo ir kad mastas, kuriuo biometrinio atpažinimo technologijos gali pagerinti mūsų gyvenimo kokybę, priklausys nuo to, kaip mes būsime pasirengę integruoti į šias sistemas ir technologijas tiek įstatymines, tiek technologines kontrolės priemones.

Kaip matyti iš aptartų EPBO dokumentų asmens duomenų saugos, susijusios su informacinių ir biometrinių technologijų naudojimu analizės, pagrindiniai duomenų tvarkymo principai – duomenų rinkimo ir naudojimo apribojimai, kokybės, saugumo, atvirumo, individualaus dalyvavimo, atskaitomybės, informavimo apie paskirtį kriterijai buvo suformuluoti jau devintojo dešimtmečio pradžioje ir vėliau tik papildyti atsižvelgiant į technologijų raidą. Vėliausiame EPBO dokumente šie principai papildomi tik nuostatomis dėl kitų identifikavimo priemonių naudojimo galimybių įvertinimo, skatinimo naudoti periferines individualias duomenų saugyklas, naudoti autentifikavimo metodus, užtikrinti alternatyvų galimybes.

## 2. *ET konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis*

1950 m. priimtos Europos žmogaus teisių ir pagrindinių laisvių konvencijos[81] 8 str. įtvirtinus asmens teisę į privatumą, buvo padėti pagrindai asmens duomenų apsaugai. Tačiau vien tik Europos žmogaus teisių ir pagrindinių laisvių konvencijos nepakanka tinkamai ir efektyviai apsaugoti asmens duomenis, todėl prireikė kitų instrumentų.

1981 m. Europos Taryba (ET) priėmė Konvenciją dėl asmenų apsaugos, susijusios su automatizuotu asmens duomenų apdorojimu[82] (toliau Konvencija). Pagrindinis Konvencijos tikslas yra ginti žmogaus asmeninį gyvenimą, ypač teisę į privatumą. Konvencija taikoma automatizuotoms asmens duomenų rinkmenoms[83] ir valstybinio bei privataus sektoriaus asmens duomenims automatizuotai tvarkyti. Tiesa, valstybės gali pareikšti, kad konvencijos netaikys tam

---

http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF ;Prisijungimo laikas: 2007-09-10, 2004; P. 44

[81] 1950 metų lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // http://www3.lrs.lt/cgi-bin/preps2?Condition1=114048&Condition2=; Prisijungimo laikas: 2007-10-18

[82] 1981 m. Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis (ETS Nr. 108) //Valstybės žinios. 2001, Nr. 32-1059. 2000 m. vasario 11 d. Lietuva pasirašė 1981 m. Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis 2001 m. vasario 20 d. Lietuvos Respublikos Seimas priėmė įstatymą „Dėl Konvencijos dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo“ (Žin., 2001, Nr.32-1055). 2001 m. lapkričio 8 d. Lietuva pasirašė Europos Tarybos Ministrų Komiteto 2001 m. gegužės 23 d. priimtą Konvencijos ETS Nr. 108 papildomą protokolą dėl priežiūros institucijų ir duomenų srautų, kertančių valstybės sienas

[83] Automatizuota duomenų rinkmena - tai automatizuotai tvarkomų duomenų rinkinys.

tikroms automatizuotoms asmens duomenų rinkmenoms. Konvenciją sudaro trys dalys – bendrieji asmens duomenų apsaugos principai; specialios taisyklės dėl tarptautinio asmens duomenų judėjimo; tarpusavio pagalbos tarp valstybių narių užtikrinimo ir įgyvendinimo mechanizmas.

Europos Tarybos Konvencija taikoma automatizuotoms asmens duomenų rinkmenoms ir valstybinio bei privataus sektoriaus asmens duomenims automatizuotai tvarkyti. Tiesa, valstybės gali pareikšti, kad konvencijos netaikys tam tikroms automatizuotoms asmens duomenų rinkmenoms.

Pagrindiniai asmens duomenų apsaugos principai panašūs į EBPO Gairių, bet papildomai įtraukia principą, reikalaujantį atitinkamų apsaugos priemonių specialioms asmens duomenų kategorijoms (jautriems duomenims), kurie atskleidžia rasinę kilmę, politinius įsitikinimus ar religines nuostatas ar kitus įsitikinimus, kurie liečia sveikatą, seksualinį gyvenimą, ar kurie susiję su kriminaliniais nuteisimais.[84] Užtikrinant asmens duomenų apsaugą, pabrėžiama būtinybė imtis tinkamų apsaugos priemonių, kurios neleistų jų netyčia ar neteisėtai sunaikinti, prarasti, neleistinai palikti juos prieinamus, keisti ar platinti.[85]

**Vykdomas darbas.** Per Konsultacinį komitetą Europos Taryba tęsia pradėtą darbą asmens duomenų apsaugos srityje. Pažymėtina, kad galima išskirti keletą daugiau ar mažiau su biometrija susijusių Europos Tarybos Konvencijos taikymo sričių, kurioms yra pateikta nemaža ataskaitų ir rekomendacijų:

- 1987 m. rekomendacija „Dėl asmens duomenų naudojimo policijos sektoriuje“ ir vėliaus sekusios trys įvertinimo ataskaitos;
- 1989 m. rekomendacija „Dėl asmens duomenų, naudojamų įdarbinimo tikslais, apsaugos“ ir po to sekęs aiškinamasis memorandumas.
- 1991 m. rekomendacija „Dėl valstybės institucijų turimų asmeninių duomenų perdavimo trečioms šalims“ ir po to sekęs aiškinamasis memorandumas.
- 1997 m. rekomendacija „Dėl medicininių duomenų apsaugos“ ir po to sekęs aiškinamasis memorandumas.
- 2003 m. ataskaitą „Dėl asmenų apsaugos pagrindinių principų ryšium su duomenų rinkimu ir tvarkymu vaizdo stebėjimo priemonėmis.“
- 2003 m. pagrindiniai principai „Dėl asmens duomenų apsaugos protingosiose kortelėse.“
- 1991 m. studija dėl asmens kodų įdiegimo ir panaudojimo: duomenų apsaugos aspektai.

Visgi, vienintelis tiesiogiai su biometrija ir jos technologijomis sietinas šaltinis yra 2005

[84] 1981 m. Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis (ETS Nr. 108) //Valstybės žinios. 2001, Nr. 32-1059., 6 straipsnis.
[85] Ten pat, 7 straipsnis.

m. Europos Tarybos pažangos ataskaita dėl Konvencijos 108 principų taikymo biometrinių duomenų rinkimui ir tvarkymui[86] (toliau – Atskaita).

Ataskaitos tikslas – prisijungti prie diskusijų apie biometrinių duomenų apribojimą ir apsaugą. Dokumente nėra suformuojamos galutinės išvados. Konsultacinis komitetas, rengiąs šią Ataskaitą, nutarė apsiriboti pažangos ataskaita, nes kaip teigiama jos įžanginėje dalyje „dar nėra pasirengta galutiniams sprendimams“ – daug klausimų dar yra atviri svarstymams. Kaip teigiama Ataskaitoje: „pastebėti privalumai gali turėti trukumų, kurie dar nėra ištirti“, o kai kurie nuogąstavimai gali pasirodyti nepagrįstais.“ Ataskaita rekomenduoja imtis atsargumo priemonių, kad būtų išvengta galimų nepageidaujamų plėtojimosi krypčių, kurios turi didelių trūkumų asmens duomenų apsaugos atžvilgiu.

Ataskaitoje suformuluojamos tokios išvados:

1. Biometriniai duomenys turi būti laikomi specifine duomenų kategorija, kadangi jų gavimo šaltinis yra žmogaus kūnas, jie išlieka tokie pat įvairiose sistemose ir iš esmės nekinta visą gyvenimą. Tačiau jie gali pasikeisti, pavyzdžiui, dėl senėjimo, ligos arba chirurginių intervencijų.

2. Prieš griebdamasis biometrijos, kontrolierius turėtų subalansuoti, viena vertus, galimus jos privalumus ir trūkumus duomenų subjekto privačiam gyvenimui ir, kita vertus, numatytus tikslus, apsvarstyti galimas alternatyvas, turinčias silpnesnį nepageidautiną poveikį privačiam gyvenimui.

3. Biometrijos nevertėtų rinktis vien tik patogumo tikslais. Biometrijos naudojimas gali daryti poveikį žmogaus orumui. Taip pat reikėtų atsižvelgti į sociokultūrinius aspektus bei galimą nenorą naudoti žmogaus kūną, kaip instrumentą.

4. Biometriniai ir susiję duomenys, generuojami sistemos, turi būti apdorojami specifiniais, aiškiai apibrėžtais bei teisėtais tikslais ir negali būti apdorojami jokiais kitais tikslais, kurie būtų nesuderinamais su paminėtais.

5. Duomenys turi būti adekvatūs, tiesiogiai susiję ir neviršijantys šių tikslų. Techninė sistema, naudojanti biometrinius duomenis, turi būti sukonfigūruota taip, kad nebūtų galimybės kaupti daugiau biometrinių arba susijusių duomenų, negu yra būtina apdorojimo tikslais. Jeigu šablonai yra pakankami, reikėtų vengti nuotraukų rinkimo ir kaupimo.

6. Rinkdamasis sistemos architektūrą kontrolierius turėtų pasverti, viena vertus, jos privalumus ir trūkumus duomenų subjekto privačiam gyvenimui ir, kita vertus, numatytus tikslus. Atsižvelgiant į duomenų saugos aspektus reikėtų protingai rinktis duomenų laikymo būdą: tik atskiroje atmeniojoje terpėje, decentralizuotoje duomenų bazėje arba centrinėje duomenų bazėje.

[86] 2005m. Europos Tarybos pažangos ataskaita dėl Konvencijos 108 principų taikymo biometrinių duomenų rinkimui ir tvarkymui // http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/reports_and_studies_of_data_protection_committees/O-Biometrics(2005)_en.asp#TopOfPage; Prisijungimo laikas: 2007-10-19.

7. Biometrinės sistemos architektūra neturėtų būti neproporcinga duomenų apdorojimo tikslams. Todėl, jeigu verifikacija tenkina, kontrolierius neturėtų ieškoti identifikavimo sprendimų. Biometriniai duomenys, naudojami tik verifikavimo tikslais, pageidautinai turėtų būti laikomi tik atskiroje apsaugotoje atmeniojoje terpėje, pvz., intelektualiojoje kortelėje, kurią turėtų tik duomenų subjektas.

8. Duomenų subjektas turi būti informuojamas apie sistemos tikslus ir kontrolieriaus tapatybę, nebent jam arba jai tai jau būtų žinoma, taip pat apie apdorojamus asmens duomenis bei asmenis arba asmenų kategorijas, kurioms jie bus atskleisti tokiu mastu, kokiu ši informacija reikalinga apdorojimo teisingumo užtikrinimui.

9. Duomenų subjektas turi teisę gauti, taisyti, užblokuoti ir sunaikinti su juo arba su ja susijusius duomenis. Šios teisės apima biometrinius duomenis, kuriems taikomas automatinis apdorojimas, susijęs su tapatybe, taip pat galimus susijusius duomenis (pavyzdžiui, sistemos naudojimo datą ir vietą) bei asmenis, kuriems jie yra perduodami.

10. Kontrolierius turi numatyti adekvačias technines ir organizacines priemones, kurių tikslas apsaugoti biometrinius ir susijusius duomenis nuo atsitiktinio arba tyčinio sunaikinimo arba praradimo, taip pat nuo neteisėtos prieigos, pakeitimo, perdavimo neautorizuotiems asmenims arba kitų neteisėto apdorojimo formų.

11. Sertifikavimo, monitoringo ir kontrolės sistema, jeigu ji nustatyta nepriklausomos institucijos, turi būti viešai skelbiama, ypač masinio naudojimo atvejais, atsižvelgiant į programinės, techninės įrangos kokybės standartus bei atsakingų už registraciją ir palyginimą darbuotojų parengimo reikalavimus. Rekomenduojama periodiškai atlikti sistemos veikimo patikrinimus.

12. Jeigu naudojant biometrinę sistemą duomenų subjektas buvo atmestas, jam arba jai pareikalavus kontrolierius privalo atlikti pakartotinį patikrinimą ir, prireikus, pasiūlyti tinkamą alternatyvų sprendimą. Procedūros turi būti tinkamos ir žinomos duomenų subjektui tuo atveju, jeigu sistema pateiktų tariamai klaidingą rezultatą.

Apibendrinant reikia pasakyti, kad nepaisant žymių technologinių laimėjimų po Konvencijos projekto parengimo, yra pripažįstama, kad Konvencijoje nustatyti principai tebėra aktualūs taip pat ir biometrinėms sistemoms. Ataskaita atspindi teisės principų suderinamumą su šiomis naujomis technologijomis. Jos tikslas prisidėti prie debatų dėl žmogaus teisių ir biometrijos santykio, nuolat vykstančių tiek tarptautiniame, tiek nacionaliniame lygmenyje. Taip pat reikia pažymėti, šioje ataskaitoje užsimenama, kad ET išleis naujas ataskaitas, atnaujins pastarąją arba sukurs naujas teisines priemones nedelsiant, kai tik to pareikalaus biometrinių technologijų plėtra.

## *3. Biometrijos teisinis reglamentavimas Europos Sąjungos duomenų apsaugos politikos kontekste*

Europos Sąjungos teisėje ilgą laiką nebuvo specialaus dokumento, reglamentuojančio žmogaus teisių apsaugą. Europos Bendrija buvo linkusi palaukti kol išaiškės asmens duomenų apsaugos teisinio reguliavimo tendencijos tarptautiniu lygmeniu. Net ir Europos Tarybai 1981 m.. priėmus Konvenciją dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis (ETS Nr. 108) ir 1980 m. EBPO patvirtinus Asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gaires, ES savo atsaką pateikė tik 1995 m., direktyva 95/46/EB Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Direktyva) įtvirtinus ES asmens duomenų apsaugos režimą.

### 3.1. Asmens duomenų apsauga biometrijos kontekste pagal Europos Sąjungos teisę

Direktyva 95/46/EB siekiama harmonizuoti valstybių narių nacionalinius teisės aktus ir įgyvendinti dvejopo pobūdžio tikslus – iš vienos pusės apsaugoti fizinių asmenų pagrindines teises ir laisves, o ypač jų teisę į privatumą tvarkant asmens duomenis, o iš kitos pusės – nevaržyti laisvo asmenų duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga[87]. Direktyva siekia užtikrinti Europos žmogaus teisių ir pagrindinių laisvių konvencijoje įtvirtintų esminių žmogaus teisių, kaip visuotinai pripažįstamų socialinių vertybių, apsaugą. Tai matyti iš tokių Direktyvos nuostatų: "asmens duomenų tvarkymą reglamentuojančių nacionalinių įstatymų tikslas - apsaugoti pagrindines teises ir laisves, ypač privatumo teisę, ir tai pripažįstama Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje, taip pat Bendrijos teisės aktų bendruosiuose principuose"[88]. Taigi, galima teigti, kad Europos Sąjungos asmens duomenų apsaugos kilmė – bendroji tarptautinė teisė. Kaip žinia, Europos žmogaus teisių ir pagrindinių laisvių konvencija nustato bendruosius Europos Sąjungos teisės principus, nes tai

[87] Direktyvos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15; 1 straipsnis.

[88] Direktyvos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15; 10 įžanginė citata.

įtvirtinta 1992 m. Europos Sąjungos Steigimo Sutarties[89] (Mastrichto sutarties) F straipsnio 2 dalyje.

Direktyva išreiškia Europos Sąjungos institucijų susirūpinimą tuo, jog asmens duomenų rinkimas, kaupimas, tvarkymas tampa kasdieniniu reiškiniu daugelyje ekonominių ir socialinių sferų. Tuo pačiu informacinių technologijų vystymasis ypatingai pagreitina asmens duomenų rinkimą ir perdavimą[90].

Skirtingi nacionaliniai asmens duomenų apsaugos režimai gali tapti viena pagrindinių kliūčių sklandžiam asmens duomenų judėjimui, todėl Direktyva siekiama visose valstybėse narėse įtvirtinti visuotinai privalomą asmens duomenų apsaugos minimumą tokiu būdu garantuojant efektyvų Europos Bendrijos vidaus rinkos funkcionavimą, pagrįstą netrukdomu asmens duomenų judėjimu[91]. Suvienodinus valstybių narių įstatymus asmens duomenų apsaugos srityje visoje Europos Bendrijos vidaus rinkoje bus pasiektas ekvivalentiškas asmens duomenų apsaugos lygis ir valstybės narės nebegalės riboti asmens duomenų judėjimo pagrindais, susijusias su žmogaus teisių, žmogaus teisės į privatumą, apsauga[92].

Direktyva kartu su Europos Tarybos 1981 m. Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis ir 1980 m. EBPO Asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairėmis nustato teisinį biometrinių technologijų Europoje pagrindą.[93]

## 3.2. Direktyvos 95/46/EB taikymas biometrijai

Direktyvos 95/46/EB 3 (1) straipsnis nustato, kad Direktyva taikoma *automatiniais būdais tvarkant asmens duomenis ištisai arba dalimis*. Taigi, kaip matyti, Direktyvos rengėjai siekė, kad į jos reguliavimo sritį patektų visos įmanomos automatinio asmens duomenų rinkimo ir tvarkymo formos, net ir tos, kurios akivaizdžiai neegzistavo jos priėmimo metu. Todėl pacituotas straipsnis suformuluotas tokiu būdu, kad apimtų tiek egzistuojančias, tiek ir bet kokias ateities technologijas, įgalinančias automatinį, tai yra ne rankinį, duomenų rinkimą ir tvarkymą. Taigi,

[89] 1992 metų Europos Sąjungos Sutartis (Mastrichto sutartis) // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=32156 ; Prisijungimo laikas: 2007-11-15.
[90] Direktyvos 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15; 4 įžanginė citata.
[91] Ten pat, 7 įžanginė citata.
[92] Ten pat, 9 įžanginė citata.
[93] Direktyva 95/46/EB taip pat papildo: 1) 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo; 2) 2002 Europos Parlamento ir Tarybos direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“.

remiantis išdėstytu, galima daryti išvadą, kad biometrija patenka į direktyvos taikymo sritį. Kartu direktyvos 3 (2) straipsnis nustato, kad *Direktyva netaikoma tvarkant asmens duomenis, kai duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine ar namų ūkio veikla*.

Taigi Direktyva netaikoma išimtinai asmeninėje veikloje, net kai ji susijusi su asmeniniais duomenimis. Be abejo, kai kurie autentiškumo nustatymo būdai naudojant biometrinius duomenis, gali būti laikomi tokia veikla. Pavyzdžiui, kortelėse įrašyti piršto antspaudai. Šiuo atveju piršto atspaudas niekada nėra perduodamas be kortelės – nei kai informacija iš pradžių įrašoma, nei kai ji yra naudojama. Kortelė tik atsako „taip arba „ne“ į klausimą, ar tinkamas asmuo turi kortelę. Tai gali būti palyginta su atveju, kai su savo raktu patenkame į namus. Tokiu atveju svarstytina, ar asmeniniai duomenys tebepriklauso tam asmeniui.

Direktyvos 95/46/EB 2 straipsnio a) dalis terminą *"asmens duomenys*" apibrėžia *kaip bet kokią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais.*

Pagal šį apibrėžimą biometriniai duomenys visuomet gali būti laikomi „*informacija, susijusia su asmeniu*”, kadangi tai yra duomenys, kurie savo prigimties dėka suteikia informacijos apie tam tikrą asmenį.

Tapatybės nustatymo naudojant biometrinę sistemą kontekste taip pat galima teigti, kad asmens tapatybė gali būti nustatyta, nes identifikavimo procese naudojant asmens biometrines charakteristikas tam tikras asmuo yra išskiriamas iš visų kitų asmenų. Taigi, galimybė nustatyti asmens tapatybę nepriklauso nuo kitų duomenų, kurie, naudojami kartu ar atskirai ir leidžia nustatyti jo tapatybę. Reikia taip pat pastebėti, kad tiesioginio tapatybės nustatymo galimybė naudojant vieną ar kelis to asmens fizinei tapatybei būdingus veiksnius yra aiškiai nurodyta Direktyvoje pateikiamame apibrėžime.

Ankstesnėje dalyje, kalbant apie biometrines sistemas, buvo išskirtos kelios biometrinių duomenų tvarkymo proceso stadijos. Pirmoji stadija yra asmens registracija. Vėliau vyksta tam tikrų asmens ypatybių (pvz. pirštų antspaudų) analizavimas, po to, jų įvertinimas, biometrinės informacijos atskyrimas ir jos išsaugojimas modelyje.

Nėra priežasčių, leidžiančių manyti, kad tai, kas taikoma pačiai asmens charakteristikai, nebūtų taikoma skaitmeniniam šios savybės atvaizdui, modeliams, kurie buvo sukurti tokių atvaizdų pagrindu, ir bet kokiems paskesniems pertvarkymams. Pažymėtina, kad nors detalių kiekis keičiasi, tačiau unikalus ryšys su tam tikru asmeniu išlieka. Todėl galima pagrįstai daryti išvadą, kad surinkti

duomenys išliks asmeniniai didžiojoje dalyje duomenų rinkimo stadijų. Tam, kad būtų galima nustatyti, ar Direktyva yra taikytina, reikia atsakyti į klausimą, kada asmeniniai duomenys tvarkomi, ir ar būdas, kuriuo asmeniniai duomenys yra naudojami, patenka į Direktyvos reguliavimo sritį.

Direktyvos 2(b) straipsnyje, pateikiamas termino „*tvarkymas*“ apibrėžimas yra gana platus: „asmens duomenų tvarkymas" (tvarkymas) reiškia bet kurią operaciją ar operacijų rinkinį, automatiniais arba neautomatiniais būdais atliekamą su asmens duomenimis, kaip antai: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas perduodant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas. Šiuo požiūriu, pavyzdžiui, identifikacija (tapatybės nustatymas) naudojant biometrinius duomenis gali apimti asmeninių duomenų tvarkymą, kai yra saugomas algoritmiškai tvarkomas biometrinių duomenų elementas (pvz., biometrinių duomenų modelis).

Kitas klausimas, kurį būtina išnagrinėti, yra teisinės pasekmės, kylančios žmogaus ypatybę įvardijus asmeninių duomenų elementu, patenkančiu į Direktyvos taikymo sritį. Tokiu atveju turi būti laikomasi Direktyvos nustatytų sąlygų, t.y.:

Direktyvos 6 straipsnis nustato, kad valstybės narės numato, kad asmens duomenys turi būti:

*a) tvarkomi teisingai ir teisėtai;*

*b) surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais. Tolesnis duomenų tvarkymas istoriniais, statistiniais ar moksliniais tikslais laikomas suderinamu, su sąlyga, kad valstybės narės numato atitinkamas apsaugos priemones;*

*c) adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi;*

*d) tikslūs ir, jei būtina, nuolat atnaujinami; turi būti imtasi visų reikalingų priemonių, kad duomenys, kurie yra netikslūs ar neišsamūs, palyginti su tikslais, dėl kurių jie buvo surinkti ar po to tvarkomi, būtų ištrinti arba ištaisyti;*

*e) laikomi tokiu pavidalu, kad duomenų subjektų tapatybes būtų galima nustatyti ne ilgiau, nei tai yra reikalinga tais tikslais, dėl kurių duomenys buvo surinkti arba po surinkimo tvarkomi. Valstybės narės išdėsto asmens duomenų, kurie yra saugomi ilgesnį laiką dėl jų istorinės, statistinės ar mokslinės paskirties, atitinkamas apsaugos priemone;*.

Direktyvos 7 straipsnis nustato, kad valstybės narės numato, kad asmens duomenis galima tvarkyti tik tuo atveju, jeigu:

*a) duomenų subjektas yra nedviprasmiškai davęs sutikimą dėl duomenų tvarkymo;*

*b) tvarkyti reikia vykdant sutartį, kurią duomenų subjektas yra sudaręs kaip viena iš sutarties šalių arba duomenų subjekto reikalavimu norint imtis priemonių prieš sudarant sutartį;*

*c) tvarkyti reikia vykdant teisinę prievolę, kuri privaloma duomenų valdytojui;*

*d) tvarkyti reikia norint apsaugoti gyvybinius duomenų subjekto interesus;*

*e) tvarkyti reikia vykdant užduotį, atliekamą visuomenės labui arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui arba trečiajai šaliai, kuriai atskleidžiami duomenys; arba*

*f) tvarkyti reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kuriai atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto, kuriam pagal Direktyvos 1 straipsnio 1 dalį reikalinga apsauga, teisės ir laisvės yra viršesnės nei šie interesai.*

Direktyvos 6 (a) straipsnio nuostatos reiškia, kad duomenų tvarkymas ir rinkimas turi būti atliekamas sąžiningai. Taigi žmonės turėtų būti informuojami apie tai, kad jų tapatybė nustatoma naudojant jų biometrinius duomenis. Taip pat šiuo atžvilgiu svarbus Direktyvos 10 straipsnis (bus kalbama vėliau).

Direktyvos 6 (b) straipsnyje aptariami, asmens biometrinių duomenų, naudojamų asmens tapatybės nustatymui, tvarkymo klausimai. Sprendžiant klausimą, ar tam tikras asmuo turi teisę pasinaudoti konkrečios biometrine sistemos duomenimis, ar ne, šių duomenų naudojimas nustatant emocinę to asmens būseną ar rasę, būtų iš esmės nesuderinamas su tikslu, kurio siekiama, t.y. su biometriniu tapatybės nustatymu. Be to, sutinkamai su Direktyvos 7 straipsniu, tokių asmeninių duomenų tvarkymo tikslas turi būti pagrįstas. Duomenų tvarkymas leidžiamas, jeigu yra bent viena sąlyga iš Direktyvos 7 straipsnyje pateikiamo sąrašo.

Pagal Direktyvos 10 straipsnį duomenų valdytojas privalo nurodyti duomenų subjektui, iš kurio yra renkami su juo susiję duomenys, suteikiant bent jau šią informaciją:

*a) duomenų valdytojo arba jo atstovo, jei toks yra, tapatybė;*

*b) tikslai, dėl kurių ketinama tvarkyti šiuos duomenis;*

*c) bet kokia platesnė informacija, kaip antai:*

- *duomenų gavėjai ar gavėjų kategorijos;*
- *ar į klausimus atsakoma privaloma tvarka, ar savanoriškai, taip pat galimos neatsakymo pasekmės;*
- *teisės gauti informaciją ir teisės pataisyti duomenis apie save buvimas;*
- *kiek tokios išsamesnės informacijos reikia, atsižvelgus į specifines duomenų rinkimo aplinkybes, kad būtų garantuotas teisingas subjekto duomenų tvarkymas.*

Biometrinio tapatybės nustatymo situacijoje svarbu yra tai, kad tam tikras atpažinimo metodas negali būti naudojamas nežinant duomenų subjektui, t.y. asmeniui, kurio biometriniai duomenys yra renkami.

Direktyva taip pat reglamentuoja ir ypatingųjų duomenų tvarkymą: dokumento 8 (1) straipsniu nustatoma, jog *„Valstybės narės uždraudžia tvarkyti asmens duomenis, kurie atskleidžia rasinę ar etninę kilmę, politines, religines ar filosofines pažiūras, priklausymą profesinėms sąjungoms, taip pat [..] duomenis apie asmens sveikatą ar intymų gyvenimą“*.

Paprastai praktikoje specialios duomenų kategorijos suprantamos kaip "ypatingi duomenys“. Taigi iškyla klausimas ar gali biometriniai duomenys būti laikomi ypatingais duomenimis Direktyvos prasme ir ar jų, kaip ypatingų duomenų, traktavimas priklauso nuo faktiško biometrinių duomenų naudojimo?

Jau buvo nurodytos kelios duomenų tvarkymo stadijos. Pirmoji yra žmogaus charakteristikų „surinkimas“, įvertinimas ir biometrinio atvaizdo sukūrimas. Šioje stadijoje „neapdorotame“ arba nesutvarkytame atvaizde kartais yra informacijos, kuri gali būti tiesiogiai interpretuojama kaip informacija apie asmens rasę arba sveikatos būklę. Pavyzdžiu gali būti veido atvaizdas, iš kurio matyti odos spalva arba tam tikri ligos požymiai. Tokiais atvejais atvaizdai gali būti priskiriami ypatingiems duomenims.

Kitas žingsnis duomenų tvarkymo procese yra pirminių duomenų apdorojimas ir biometrinio modelio sukūrimas. Svarstytina, ar apdoroti duomenys tebėra priskirtini ypatingiems duomenims. Pirmiausia, labai tikėtina, kad specifinės savybės, dėl kurių duomenys laikytini ypatingais, nėra naudojamos nustatant gautus duomenis. Pavyzdžiui, kai jau nustatomas piršto atspaudo modelis, tai odos spalva, šiuo atveju bus nebeaktuali, nes jos nebegalima bus išskaityti. Antra, gali būti neįmanoma protingomis priemonėmis atkurti modelį, sukurtą pagal gautus duomenis. Šiuo atveju priskyrimas ypatingiems duomenims būtų sunkiai pagrįstas.

Specialių duomenų kategorijoms taikomi papildomi įstatymo reikalavimai. Reikalavimai, susiję su ypatingų duomenų tvarkymu, yra griežtesni. Esminė taisyklė įtvirtinta Direktyvos 8 (1) straipsnyje, kuris *draudžia* tokius duomenis tvarkyti. Direktyvos 8 (2) – 8 (4) straipsniuose pateikiami specialūs atvejai, kai šis draudimas nėra taikomas. Kiekviena valstybė narė šių išimčių įgyvendinimą detaliai apibrėžia savo nacionalinėje teisėje. Išimtys gali būti taikomos tik griežtai apibrėžtais atvejais:

*„8 (2) a) duomenų subjektas davė aiškų sutikimą tvarkyti tokius duomenis, išskyrus, kai valstybės narės įstatymai numato, kad 1 dalyje nurodyto draudimo negalima panaikinti duomenų subjekto duotu sutikimu;*

*8 (2) b) tvarkyti būtina, norint įgyvendinti duomenų valdytojo prievoles ir specifines teises darbo įstatymų srityje, kiek tai leidžia nacionalinės teisės aktai, numatantys atitinkamas apsaugos priemones;*

*8 (2) c) tvarkyti būtina, kad būtų apsaugoti duomenų subjekto arba kito asmens gyvybiniai interesai, kai duomenų subjektas fiziškai neįgali arba yra juridiškai neveiksnus duoti sutikimą;*

*8 (2) d) duomenis tvarko fondas, asociacija ar kita pelno nesiekianti organizacija politiniais, filosofiniais, religiniais ar su profesinėmis sąjungomis susijusiais tikslais savo teisėta veikla su atitinkamomis garantijomis ir su sąlyga, kad taip tvarkomi duomenys yra susiję tiktai su tos organizacijos nariais arba su asmenimis, kurie reguliariai palaiko ryšius su šia organizacija dėl jos siekiamų tikslų, ir kad tokie duomenys nėra atskleidžiami trečiajai šaliai be duomenų subjektų sutikimo; arba*

*8 (2) e) tvarkomi tokie duomenys, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai arba kurie yra reikalingi nustatyti, įvykdyti ar apginti teisinius ieškinius.*

*8 (3) Šio straipsnio 1 dalis netaikoma, kai duomenis reikia tvarkyti teikiant profilaktines medicinos, medicininės diagnostikos, medicinos priežiūros, gydymo, sveikatos apsaugos paslaugas ir kai tokius duomenis tvarko sveikatos apsaugos darbuotojas, kuriam pagal nacionalinius įstatymus arba nacionalinių kompetentingų institucijų nustatytas taisykles galioja profesinės paslapties saugojimo pareiga, arba kitas asmuo, kuriam irgi galioja lygiavertė paslapties saugojimo prievolė.*

*8 (4) Dėl svarbių visuomenės interesų valstybės narės greta šio straipsnio 2 dalyje išdėstytų išimčių nacionaliniais įstatymais ar priežiūros institucijų sprendimais gali numatyti kitas išimtis, bet turi užtikrinti tinkamas apsaugos priemones“.*

*„Sutikimo davimas“, kaip numatyta Direktyvos 8(2) (a) straipsnyje, turėtų atitikti apibrėžimą, pateiktą Direktyvos 2 (h) straipsnyje: "duomenų subjekto sutikimas" reiškia bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys“.*

Apibendrinant pasakytina, kad sistemoms, naudojančioms biometrinę identifikaciją (tapatybės nustatymą) arba autentifikavimą (tapatybės patvirtinimą), šios privalomos sąlygos yra pagrindinės. Jeigu neapdoroti arba tvarkomi duomenys yra laikomi ypatingais duomenimis, jų tvarkymas iš esmės yra draudžiamas. Kai kuriais atvejais duomenų tvarkymas gali būti pateisinamas, jeigu yra duotas aiškus sutikimas. Skirtingų duomenų tvarkymo stadijų analizė rodo, kad dažnai tik neapdoroti duomenys gali būti priskiriami ypatingiems duomenims. Tokie duomenys apskritai negali būti saugomi. Tačiau jeigu šie duomenys ir yra pašalinami, sunku užtikrinti, kad draudimo juos tvarkyti bus laikomasi vėliau.

Šioje vietoje reikėtų paminėti ypatingą atvejį - kai atsiranda naujos programos (pvz. biometrinių pasų), įpareigojančios piliečius pateikti savo biometrines charakteristikas. Jeigu šie biometriniai duomenys yra priskiriami ypatingiems ir vėliau yra saugomi duomenų bazėse,

reikalavimas gauti piliečių sutikimą, aukščiau apibrėžtą kaip „savanoriškai ir žinomai duotą pareiškimą", netaikomas. Šiuo atveju gali būti tikslinga priimti atitinkamus naujus teisės normas.

Direktyvos 17 straipsnis reikalauja, jog duomenų valdytojas (asmuo arba institucija, kuri nustato tikslus ir priemones, skirtas asmeninių duomenų apdorojimui) realizuotų tinkamas technines ir organizacines priemones tam, kad apsaugotų asmeninius duomenis. Reikalaujama, jog duomenų valdytojas privalo įgyvendinti apsaugos priemones nuo:

- *netyčinio ir neteisėto sunaikinimo ar netyčinio praradimo;*
- *pakeitimo;*
- *neleistino atskleidimo ar palikimo prieinamais;*
- *visų kitų neteisėtų apdorojimo priemonių*.

Ypatingai tai taikoma atvejams, kai tvarkomus duomenis tenka perduoti tinklu. Saugumo priemonės gali būti sudarytos iš, pavyzdžiui, modelių šifravimo ir šifravimo raktų apsaugos[94], papildant prieigos kontrolę ir apsaugą, kad būtų neįmanoma iš modelių atkurti pradinius duomenis.

Būtinos saugumo priemonės turi būti įgyvendintos tvarkymo pradžioje ir ypač „registracijos" fazėje, kur biometriniai duomenys yra paverčiami modeliais ar vaizdais. Reikia suprasti, „kad bet koks integralumo, konfidencialumo ir tinkamumo principų nepaisymas duomenų bazėse būtų aiškiai žalingas visiems būsimiems pritaikymams, besiremiantiems tokiose duomenų bazėse turima informacija, ir padarytų nepataisomą žalą duomenų subjektams."[95] Galima tokia situacija, kai asmens pirštų atspaudai būtų susieti su neįgalioto asmens tapatybe, pastarasis gali naudotis paslaugomis, prieinamomis pirštų atspaudų savininkui, neturėdamas tam teisės. Tai galėtų būti traktuojama kaip tapatybės vagystė ir, pirštų atspaudai taptų nepatikimais būsimiems taikymams, tokiu būdu būtų ribojama asmens laisvė. Biometrinėse sistemose pasitaikančios klaidos asmens duomenų subjektams gali turėti kelias pasekmes: klaidingas įgalioto asmens atmetimas ir klaidingas neįgalioto asmens priėmimas gali sukurti rimtų, įvairaus lygio problemų. Tokiais atvejais, bet koks sprendimas, kuris teisiškai paveikia subjektą, turi būti priimamas tik po pakartotinio automatinio tvarkymo rezultato patvirtinimo pagal Direktyvos 95/46/EB 15 straipsnį.

[94] Tai sąlygoja mažesnę grėsmę duomenų subjektui, kadangi duomenys gali būti iššifruojami tik naudojant naują duomenų subjekto biometrinių duomenų rinkinį ir tokiu būdu išvengiama sukūrimo duomenų bazių, kaupiančių biometrinių duomenų modelius, kurie potencialiai gali būti pakartotinai panaudojami nesusijusiais tikslais.

[95] Direktyvos 95/46/EB 29 str. darbo grupės 2001 m. rugsėjo 13 d. Darbinis dokumentas Nr. 12168/02, WP 80 „Dėl biometrinių duomenų"// http://www.ada.lt/images/cms/File/WP80.pdf; Prisijungimo laikas: 2007-10-15.

## 3.3. Tikslingumo ir proporcingumo principas

Kaip buvo minėta, 29 straipsnio Darbo grupė konstatavo, kad tikslingumo ir proporcingumo principas yra vienas svarbiausių principų nagrinėjant biometrines sistemas. Darbo grupė asmenų apsaugai tvarkant asmens duomenis rėmėsi Direktyvos 95/46/EB 6 straipsniu, kuris įtvirtina reikalavimą, kad *„(...)asmens duomenys turi būti: a) tvarkomi teisingai ir teisėtai; b) surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais (…)”* ir būti *“adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi (…)”*. Tačiau Darbo Grupė savo išvadoje dėl biometrinių duomenų pateikia mažai informacijos apie tai, kaip tikslingumo ir proporcingumo principas turėtų būti taikomas biometrinių duomenų atžvilgiu. Išvadoje naudojama bendra sąvoka „teisingai“ yra neapibrėžta ir plati. Galima daryti išvadą, kad tinkamas duomenų apdorojimo procesas nepagrįstai nesikėsina į asmens privatumą, autonomiją ir vientisumą ir yra aiškus[96].

„Teisėta“ yra sąvoka, reiškianti tai, kad apdorojimas neturi prieštarauti duomenų apsaugos įstatymams, kitiems teisės aktams ar teisės principams. Tačiau kuriais atvejais biometrinių duomenų apdorojimas yra „teisingas ir teisėtas“, nėra aiškiai nurodyta. Dar neaiškiau yra apibrėžta duomenų apdorojimo proporcingumo proporcingas galimoms grėsmėms sąvoka.

Darbo Grupė savo išvadoje pasisakė apie biometrinių duomenų naudojimą patekimo kontrolės tikslais ir pareiškė, kad būdas, kuris galėtų būti naudojamas biometriniams duomenims saugoti, t.y, centralizuotai ar pagal objektus (pvz. kortelė su įrašytais pirštų antspaudais), kontroliuojamus duomenų subjekto, nustatys asmens teisėms kylančių grėsmių dydį. Biometrinių duomenų saugojimas centrinėje duomenų saugykloje kelia daugiau grėsmių, ypač dėl „funkcijos deformacijos“ ir informacijos susiejimas keliose duomenų bazėse. Tuo pačiu metu Darbo Grupė pareiškė, kad toks duomenų saugojimas centriniu lygiu yra leistinas padidinto saugumo pastatuose, iš anksto suderinus su nacionalinėmis duomenų apsaugos institucijomis. Kiti kriterijai, kurie gali būti aktualūs nustatant proporcingumo laipsnį, yra biometrinių duomenų rūšis, (pvz., delno kontūro naudojimas vietoj pirštų atspaudų) ir būdas, kaip biometriniai duomenys yra užkoduoti. Kriterijai sprendimo priėmimui dėl biometrinių duomenų naudojimo proporcingumo, nėra aiškūs. Šie kriterijai taip pat nenustatyti Direktyvoje.

[96] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. // http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-11-15; 38 įžanginė citata: susieja teisingumo sąvoką su aiškumu ir informacija.

Savo veikloje Europos Sąjungos valstybių narių duomenų apsaugos institucijos patvirtino, kad tikslo ir proporcingumo principai yra svarbiausi. Šiuo atveju pagrindinis vaidmuo tenka duomenų apsaugos institucijos bei teismams, tikrinantiems ar biometrinės atpažinimo technikos naudojimas yra teisėtas ir ar atitinka jos taikymo tikslus, numatytus direktyvoje 95/46/EB. Tačiau kriterijai, kuriais remiasi duomenų apsaugos institucijos, skiriasi. Duomenų apsaugos institucijos taip pat nevienodai taiko reikalavimus, išplėtotus jų priimamuose sprendimuose. Dar daugiau – skirtingų valstybių duomenų apsaugos institucijos priima skirtingus sprendimus arba užima skirtingas pozicijas panašių biometrinių sistemų atžvilgiu. Pavyzdžiui, biometrinių duomenų naudojimas kelionėse oru: 2003 m. lapkričio 5 d. Graikijos duomenų apsaugos institucija priėmė neigiamą sprendimą dėl rainelės ir pirštų atspaudų naudojimo keleivių lustinėse kortelėse, tuo tarpu *„Privium“* programa, naudojanti rainelės duomenis dažnų keleivių kortelėse, jau penkerius metus veikia Nyderlandų *Schiphol* oro uoste[97].

Proporcingumo principą tenka prisiminti ir derinant interesus pagal Direktyvos 95/46/EB 7 (f) straipsnį, kuris labai ribotai nurodo teisėtą pagrindą, leidžiantį apdoroti duomenis. Paskutinis pagrindas, kuriuo remiantis gali būti apdorojami asmeniniai duomenys, yra atvejai, kai duomenis „tvarkyti *reikia* dėl *teisėtų interesų*, kurių siekia duomenų valdytojas (...), išskyrus atvejus, kai duomenų subjekto, kuriam pagal 1 straipsnio 1 dalį reikalinga apsauga, *teisės ir laisvės* yra *viršesnės* nei šie interesai. 1 (1) straipsnis, kuriuo ši nuostata remiasi, įpareigoja valstybes nares užtikrinti pagrindines teises ir laisves, kai apdorojami asmeniniai duomenys, ypač - teisę į privatumą.

Teisių derinimo procese, kurio ištakos yra bendrojoje teisės sistemoje, vėl susiduriama su proporcingumo reikalavimu. Proporcingumo principas šiame kontekste remiasi bendruoju teisės principu, reikalaujančiu teisingo balanso ir pagrįstų ryšių tarp prašomų ar panaudotų priemonių, įskaitant tokių priemonių griežtumą, tęstinumą, ir tikslo, kurio yra siekiama. Principas yra kilęs iš viešosios teisės, kurioje jo paskirtis yra apsaugoti asmenis nuo valstybės kišimosi; pagrindinių žmogaus teisių užtikrinimo kontekste ir pagal precedentinę teisę, susiformavusią šioje srityje, kėsinimasis į šias teises yra draudžiamas, jei tai nėra „ nurodyta įstatymo“, nesant „teisėtų tikslų“, ir su sąlyga, kad kėsinimasis į šias teises yra „svarbus“ ar „būtinas“, ir „neviršijantis tikslų“, kurių neįmanoma pasiekti jų nepažeidžiant. Šis proporcingumo principas dabar taip pat yra taikomas

[97] Kitas pavyzdys yra 2001 m. kovo 19 d. Olandijos duomenų apsaugos institucijos išvada, susijusi su biometrine įėjimo sistema maitinimo ir sporto infrastruktūrų lankytojams, pavadinta VIS 2000. Šioje išvadoje duomenų apsaugos institucija yra pasiruošusi šios sistemos naudojimui, su sąlyga, kad kontroliuojantis asmuo įgyvendins jos devynias rekomendacijas biometrinių duomenų apdorojimui. Tačiau Belgijos duomenų apsaugos institucija savo metinėje 2005 m. ataskaitoje nurodė, kad jos nuomonė panašios biometrinės įėjimo sistemos atžvilgiu yra neigiama.

sprendžiant privačių šalių konfliktus[98]. Kriterijai, kuriais remiantis taikomas šis principas, jau plačiai svarstyti žmogaus teisių bylose, taip pat akcentuojami ir biometrinių duomenų apdorojimo kontekste. Proporcingumo principas taip pat yra susijęs su valstybių aiškinimo laisvės ribų doktrina. Egzistuoja grėsmė, kad, nesant aiškaus atsakymo, kokiais kriterijais reikia vadovautis sprendžiant, ar biometrinių duomenų apdorojimas yra teisingas ir proporcingas, ir kuris interesas nusveria kitą, duomenų apsaugos institucijos ir teismų atliekamas valstybių aiškinimo ribos ir toliau augs, o pagrindinių teisių, kurioms gali kilti grėsmė, apsaugos lygis bus nevienodas. Tačiau Darbo Grupės tikslas buvo apriboti išsiskiriančius traktavimus.

Todėl reikalingas tolimesnis tyrimas, nustatantis kokiais atvejais biometrinių duomenų apdorojimas yra teisingas ir teisėtas, ir kokie kriterijai leidžia nustatyti ar biometrinių duomenų apdorojimas yra proporcingas (teisėtam) tikslui. Šis tyrimas gali parodyti, kad dabartinis biometrinių duomenų reglamentavimas turi trūkumų ir kad šiuo atžvilgiu tikslinga imtis papildomos iniciatyvos.

## 4. Duomenų apsaugos direktyvos įgyvendinimas Europos Sąjungos valstybėse narėse

Europos Sąjungoje asmens duomenų saugumas yra siejamas su viena pagrindinių žmogaus teisių – teise į privatumą. Tačiau, reikia pažymėti ir tai, kad valstybėse narėse egzistuoja skirtumai, susiję su asmens duomenų apsaugos bei Duomenų apsaugos direktyvos įgyvendinimo tikslais ir kitais aspektais. Nors dauguma šių skirtumų nėra tiesiogiai susiję su biometrija, tačiau tam tikri, pakankamai reikšmingi, Direktyvos interpretavimo skirtumai turi poveikį biometrijos technologijų naudojimo konkrečiose srityse teisėtumui. Pagrindiniai tokio pobūdžio skirtumai sietini su šiais klausimais: kurie valstybiniai duomenų apsaugos įstatymai yra taikytini tam tikromis aplinkybėmis; ar su baudžiamąja veika susiję duomenys yra “ypatingieji duomenys”, kuriuos galima apdoroti tik gavus duomenų subjekto sutikimą; ar taikant išimtis, leidžiančias apdoroti duomenis, „jeigu tai būtina viešųjų interesų arba oficialių institucijų veiklos užtikrinimui”, reikalaujama, kad funkcija arba užduotis būtų nustatyta įstatyme. Taip pat skirtingai interpretuojamos ir pagrindinės sąvokos: pavyzdžiui, kas yra laikytinas “valdytoju”, „trečiąja šalimi”, “gavėju” ir t.t.. Pavyzdžiui, daugelis valstybių vadovaujasi baziniu Direktyvos apibrėžimu, kuris numato, kad “gavėjas” yra bet kuris

[98] Direktyvos 95/46/EB 7 (f) straipsnį, kuris taip pat taikomas, jeigu kontroliuojantis asmuo yra ne viešas subjektas.

asmuo, kuriam atskleidžiami duomenys. Danijoje ir Liuksemburge institucijos, kurios gauna duomenis tirdamos konkrečią bylą, nelaikomos gavėju.[99]

Vienas iš Direktyvos interpretavimo skirtumų, darančių tiesioginį poveikį biometrijos taikymui, yra susijęs su "asmens duomenų" apibrėžimu. Įvairiose valstybėse narėse skirtingai interpretuojama, ar duomenys laikytini "asmens duomenimis", kai turintis prieigą prie duomenų asmuo negali nustatyti duomenų subjekto tapatybės. Kai kurių valstybių narių įstatymai taiko reliatyvų požiūrį į "asmens duomenų" koncepciją ta prasme, kad duomenys laikomi asmens duomenimis tik kalbant apie tuos asmenis, kurie gali susieti duomenis su identifikuojamu asmeniu. Pavyzdžiui, Austrijos, Vokietijos, Graikijos, Nyderlandų, Portugalijos, Airijos ir Didžiosios Britanijos įstatymai numato, kad užkoduoti arba "įslaptinti naudojant slapyvardį" duomenys yra laikytini "asmens duomenimis" tik tų asmenų atžvilgiu, kurie turi prieigą tiek prie duomenų, tiek prie rakto (t.y. dekodavimo rakto), bet ne asmenims, neturintiems prieigos prie rakto. Didžiosios Britanijos įstatymas nustato, kad "asmens duomenys" yra tik tie duomenys, kurie susiję su realiu asmeniu, kurį galima identifikuoti "pagal šiuos duomenis ir kitą informaciją, kurią turi arba gali turėti duomenų kontrolierius."[100] Priešingai, Belgijoje, Danijoje, Suomijoje, Prancūzijoje, Italijoje, Ispanijoje ir Švedijoje laikomasi nuomonės, kad visi duomenys, kurie gali būti susieti su asmeniu bet kokiomis priemonėmis (net jeigu tam reikalingas dekodavimo raktas), yra "asmens duomenys." Tačiau šios valstybės yra linkusios kelti mažesnius reikalavimus tų duomenų apdorojimui, kurių negalima nedelsiant identifikuoti (t.y. dėl to, kad reikalingas dekodavimo raktas). Todėl nėra visiškai aišku, ar apskritai ir kokiomis aplinkybės duomenys, pagal kuriuos negalima visiškai arba skubiai identifikuoti konkretaus asmens (pavyzdžiui, užkoduoti biometriniai duomenys), yra laikytini susijusiais su identifikuotinu asmeniu.[101]

Kitas Direktyvos aspektas, lemiantis skirtingus rezultatus įvairiose valstybėse narėse, yra proporcingumo principo taikymas nustatant specifinių biometrinių identifikatorių naudojimą tam tikromis aplinkybėmis teisėtumą. Duomenų apsaugos institucijos privalo nuodugniai išnagrinėti biometrinio atpažinimo technologijas, atsižvelgdama į konkrečias aplinkybes ir tikslus, kuriais jos gali būti naudojamos. Pavyzdžiui, 2003 metų pabaigoje Graikijos duomenų apsaugos inspekcija pripažino neteisėta savanorišką bandomąją programą, taikytą Milano ir Atėnų tarptautiniuose oro uostuose, kurioje rainelės skenogramos ir pirštų atspaudai buvo naudojami užsiregistravusių oro

[99] Išsamią diskusiją apie teisės aktų ir jų taikymo skirtumus įvairiose valstybėse narėse galima rasti Korff, D., EC Study on Implementation of Data Protective Directive: Comparative Study of National Laws. Colchester: Human Rights Centre. September, 2002 // http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf; Prisijungimo laikas: 2007-11-14

[100] Ten pat.

[101] Ten pat.

keleivių tapatybės nustatymui.[102] Graikijos duomenų apsaugos inspekcija pripažino, kad šis tikslas gali būti pasiektas švelnesnėmis priemonėmis, būtent, parodant keleivių asmens tapatybės korteles, įlaipinimo talonus ir bilietus.[103] Tačiau kitu atveju, Graikijos duomenų apsaugos inspekcija leido naudoti delno geometriją kontroliuojant darbuotojų, atliekančių avarinius darbus metro stotyse, prieigą, įvertinusi riziką, alternatyvas ir darbuotojų privatumo teisės pažeidimo galimybę. Šiuo atveju griežto prieigos apribojimo poreikis buvo toks didelis, kad jokie kiti asmens duomenys (pvz., vardo ir pavardės naudojimas) nebuvo įrašomi, pasirinktas biometrinis metodas nepaliko jokių vadinamų "pėdsakų" bei centrinė duomenų bazė nebuvo sukurta.[104] Centrinės duomenų bazės egzistavimas ir tikimybė, kad tam biometrijos technologijos taikymas gali palikti "pėdsakus" yra dvi pagrindinės problemos, keliančios valstybių narių duomenų apsaugos institucijų susirūpinimą.

Daugelis valstybių narių taiko suvaržymus, apribojančius pirštų atspaudų duomenų bazių naudojimą įėjimo į pastatus kontrolei ir darbo užduočių monitoringui. Tuo pat metu taikomų apribojimų mastas skiraisi. Graikijoje, pavyzdžiui, pirštų atspaudų ėmimas apskritai laikomas neteisėtu, net turint duomenų subjekto sutikimą.[105] Skaitmeniniai pirštų atspaudai taip laikomi neteisėta darbuotojų atvykimo į darbą stebėsenos priemone. Graikijos duomenų apsaugos inspekcija taip pat teigia, kad pirštų atspaudų naudojimas net nacionalinėms tapatybės kortelėms viršija nustatytus duomenų subjekto identifikavimo tikslus ir gali "žeisti žmogaus orumą."[106] Nors šalyje leidžiama naudoti pirštų atspaudus prieigos kontrolei, tačiau tik išskirtinėmis aplinkybėmis, pavyzdžiui, kontroliuojant prieigą prie ypatingai saugomos arba konfidencialios informacijos.

Prancūzijos Nacionalinė informatikos ir laisvių komisija (CNIL) taip pat taiko suvaržymus skaitmeninių pirštų atspaudų, kaip prieigos kontrolės priemonės, naudojimui. CNIL, kaip ir Graikijos duomenų apsaugos inspekcija, išreiškė susirūpinimą tuo faktu, kad pirštų atspaudai gali palikti "pėdsaką", kuris gali būti panaudotas kitais, nei iš anksto numatytais tikslais.[107] CNIL yra labiau linkusi leisti naudoti prieigos kontrolei biometrinį plaštakos kontūrą arba rainelės stenogramą, nes šie prietaisai nepalieka „pėdsako" ir todėl mažiau tikėtina, kad jie gali būti nederamai panaudoti, lyginant, pavyzdžiui, su duomenų bazės sukūrimu.[108]

---

[102] Helllenic Republic Authority for the Protection of Personal Data, Biometric data in International Athens Airport, Decision 52/2003 May 11, 2003. // http://www.dpa.gr/Documents/Eng/Dec%2052%202003%20Biometrics_IAA.doc; Prisijungimo laikas: 2007-11-27.
[103] Ten pat.
[104] Ten pat.
[105] Analysis and Impact Study on Implementation of Directive 95/46/EC in Member States // ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf; Prisijungimo laikas: 2007-11-27.
[106] Ten pat.
[107] Ten pat.
[108] Pavyzdžiui, CNIL leido taikyti biometrinę prieigos kontrolę Luvre, naudojant plaštakos kontūrus. CNIL pažymėjo, kad plaštakos kontūrai, priešingai nei pirštų atspaudai, nepalieka pėdsakų ir todėl vardu ar gali būti naudojami kitais,

Kalbant apie pirštų atspaudus, CNIL apskritai mano, kad nepageidautina, jog vietos institucijos, mokyklos ir darbdaviai naudotų pirštų atspaudų duomenų bazes, nebent tai būtų būtinai reikalinga saugumo sumetimais.[109] CNIL atsisakė leisti naudoti pirštų atspaudų duomenų bazę arba biometrinę sistemą kontroliuojant įėjimą į miesto riedlenčių parką, įėjimą į studentų valgyklą ir darbuotojų darbo laiką ligoninėse. Tačiau CNIL leido naudoti pirštų atspaudų atpažinimo sistemą kontroliuojant prieigą prie valdymo prietaisų oro uostų padidinto saugumo zonose, kur biometriniai duomenys laikomi tik individualiose prieigos kortelėse, o ne centrinėje duomenų bazėje arba biometrinėse sistemose.[110] Taip pat leidžiama naudoti pirštų atspaudus, laikomus tik privačiose laikmenose, pavyzdžiui "intelektualiosiose kortelėse". Kiekvienu atskiru atveju CNIL svarsto, ar skaitmeninių pirštų atspaudų naudojimas yra proporcingas tikslui.

Italijos duomenų apsaugos institucija panašiai nagrinėja proporcingumo klausimus, nustatant biometrinių duomenų naudojimo prieigos kontrolei teisėtumą. Pavyzdžiui, pastaruoju metu priimdama sprendimą Italijos duomenų apsaugos institucija nustatė, kad skaitmeninių pirštų atspaudų naudojimas bankų institucijose prie įėjimo į banką viešosios prieigos monitoringo tikslais nėra proporcingas, kadangi tuo tikslu gali būti naudojamos "mažiau žeidžiančios privatumą" prieigos kontrolės sistemos.[111]

Olandijos duomenų apsaugos institucijos pripažino poreikį apdoroti biometrinius duomenis, naudojamus prieigos kontrolei, pavyzdžiui, į sporto renginius. Tačiau neleido šiuo tikslu naudoti veido atpažinimo sistemų. Vienu atveju Olandijos duomenų apsaugos institucija nurodė, kad skaitmeninis veido atvaizdas, priešingai nei pirštų atspaudai, atskleidžia pažeidžiamą informaciją apie asmens rasę, lytį ir pan. ir todėl ją galima apdoroti tik tuomet, kai tai būtina daryti duomenų subjekto identifikavimo tikslais arba gavus duomenų subjekto sutikimą.[112]

Valstybėse narėse taikomas skirtingas požiūris į tai, ar apskritai ir kada būtent duomenų apdorojimas (įskaitant biometrinius duomenis), atskleidžiantis "pažeidžiamas" ypatybes, pavyzdžiui, rasę ir t.t., yra laikytinas "pažeidžiamais duomenimis", atsižvelgiant į konkrečią Direktyvos garantuojamą apsaugą.[113] Pavyzdžiui, kaip jau buvo minėta, Olandijos duomenų apsaugos institucija mano, kad skaitmeninis veido atvaizdas, kaip įėjimo į sporto renginius

---

nesankcionuotais tikslais. Panašiai restorano mokykloje biometrinei prieigos kontrolei buvo leista naudoti plaštakos kontūrus, bet ne pirštų atspaudus.

[109] Analysis and Impact Study on Implementation of Directive 95/46/EC in Member States // ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf; Prisijungimo laikas: 2007-11-27.

[110] Ten pat.

[111] Ten pat.

[112] Analysis and Impact Study on Implementation of Directive 95/46/EC in Member States // ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf; Prisijungimo laikas: 2007-11-27.

[113] Ten pat.

biometrinės kontrolės priemonės, naudojimas sukuria pažeidžiamus duomenis Direktyvos nustatyta prasme. Olandijos Teisingumo ministerijos nuostatose teigiama, kad nuotraukos darbuotojų pažymėjimuose gali atskleisti darbuotojo rasę ir todėl yra laikytina pažeidžiamais duomenimis. Priešingai, Belgijos institucija mano, kad informacija apie etninę kilmę arba sveikatą nebūtinai yra laikytina pažeidžiamais duomenimis, jeigu ši informacija buvo sukurta įvairiais priežiūros tikslais. Tačiau jeigu tikslas yra sistemingai kaupti ir įrašinėti informaciją pagal pažeidžiamumo kriterijų, tai bus laikoma "pažeidžiamų duomenų apdorojimu." Panašiai Švedijos duomenų apsaugos institucija mano, kad nuotraukos, vaizduojančios žmonės „įprastinėse" situacijose, neturi būti klasifikuojamos kaip "pažeidžiami duomenys." Graikijoje DNR analizė baudžiamųjų bylų tyrimo tikslais atliekamą apibūdina kaip genetinius "pažeidžiamus duomenis", kadangi jie atskleidžia rasinę ir/arba etninę kilmę. Graikijos duomenų apsaugos inspekcija nustato, kad būtent todėl genetinės analizės taikymas turi apsiriboti "ypač sunkiais nusikaltimais."[114]

[114] Ten pat.

## III. Biometriniai pasai Europos Sąjungoje

2004 m. gruodžio 13 d. Europos Taryba priėmė Reglamentą dėl ES piliečių pasų apsauginių savybių ir biometrijos standartų.[115] Pagal reglamento 6 straipsnį[116], išsprendusios techninius klausimus[117], valstybės narės ne vėliaus nei per 18 mėnesių į pasus privalo įtraukti biometrinį veido atvaizdą, o vėliau - dar 18 mėnesių[118] įdiegti pirštų atspaudų sistemą. Lietuva, kaip ir daugelis Europos Sąjungos narių, biometrinius pasus pradėjo išdavinėti 2006 metų vasarą.

Privalomas (beveik)[119] visoms Europos Sąjungos narėms reglamentas, nustatęs biometrinių dokumentų įvedimą, biometrinių duomenų saugojimo būdą, paliko valstybių narių nuožiūrai spręsti ar saugoti duomenis tik asmens dokumentuose ar taip pat ir gyventojų registruose. 2006 metais Seime buvo priimti Paso[120], Tarnybinio paso[121] ir Gyventojų registro[122] įstatymo pakeitimo ir papildymo įstatymai, kurie nustatė biometrinių duomenų (skaitmeniniai veido atvaizdai bei pirštų atspaudai) pasuose naudojimą ir jų kaupimą bei saugojimą Gyventojų registre. Tas pačias teisės normas priėmė ar dar priims ir kitos Europos Sąjungos narės.

---

[115] 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004, dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų. // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:LT:HTML; Prisijungimo laikas 2007-10-12.

[116] Įsigaliojo 2005 m. sausio 18 d.

[117] Viešai ES pasų techniniai standartai dar nėra įsigalioja, visgi juos galima rasti Europos komisijos tinklalapyje. 2006 birželio 28 d. Komisijos sprendimas K(2006) 2909 nustatantis valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų technines specifikacijas, pateikiamas tinklalapyje http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_lt.pdf; Prisijungimo laikas 2007-10-12.

[118] Paskutinis terminas 2008 metų vasaris 28 d.

[119] D. Britanija (pagal 2000 m. gegužės 29 d. Tarybos sprendimą Nr. 2000/365/EB) ir Airija (pagal 2002 m. vasario 28 d. Tarybos sprendimą Nr. 2002/192/EB) nedalyvavo priimant šį reglamentą, dėl to neprivalo jo laikytis, ir jis neturi būti joms taikomas. Nežiūrint į tai tiek D. Britanijos, tiek ir Airijos biometriniai pasai, bus susieti su Europos Sąjungos reikalavimais, remiantis "Introduction of ePassports. Report by the Comptroller and Auditor General". // http://www.nao.org.uk/pn/06-07/0607152.htm; Prisijungimo laikas 2007-10-12.

[120] Paso įstatymo 1 ir 4 straipsnių pakeitimo ir papildymo bei įstatymo papildymu priedu įstatymas. // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=279763; Prisijungimo laikas 2007-10-12.

[121] Tarnybinio paso įstatymo 1, 5 straipsnių pakeitimo ir papildymo bei įstatymo papildymo priedu įstatymas. // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=279764; Prisijungimo laikas 2007-10-12.

[122] Gyventojų registro įstatymo 4, 9, 11 straipsnių pakeitimo ir papildymo įstatymas. // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=277499; Prisijungimo laikas 2007-10-12.

### *1. Tarybos Reglamentas (EB) Nr. 2252/2004*

Biometrinių pasų naudojimas Europos Sąjungoje yra numatomas Tarybos Reglamentu (EB) Nr. 2252/2004 (toliau – Reglamentas)[123]. Šis trumpas dokumentas yra taikomas valstybių narių išduodamiems pasams ir kelionės dokumentams (1 straipsnio 3 dalis), tačiau netaikomas asmens tapatybės kortelėms, nes jos nepatenka į Europos Sąjungos kompetencijos sritį[124] bei kitiems nacionaliniams dokumentams, galiojantiems mažiau nei 12 mėnesių.

Reglamentu nustatoma, jog valstybių narių išduodami pasai ir kelionės dokumentai turi atitikti jo priede pateikiamus minimalius standartus. Kartu numatoma, jog „Pasuose ir kelionės dokumentuose turi būti laikmena, kurioje yra veido atvaizdas. Valstybės narės į sąveikias formas taip pat įtraukia pirštų atspaudus.“[125] Paskutinė formuluotė reiškia, kad nors dar nėra nustatytas pirštų antspaudų biometrinio modelio standartas, tačiau ši norma nustato, kad valstybės narės ateityje turės į biometrinius pasus įtraukti pirštų antspaudus. Reglamento 1 straipsnio 2 dalis taip pat numato reikalavimus, kad „duomenys turi būti apsaugoti, o laikmena turi būti pakankamos talpos ir galios, kad būtų garantuotas duomenų integralumas, autentiškumas ir konfidencialumas.“ Ši norma neturi būti suvokiama tik kaip apibūdinanti techninius RFID lusto reikalavimus, jos reikšmė daug platesnė – tai sąlyga nustatanti privalomus įpareigojimus užtikrinti duomenų saugumą nustatytu būdu. Tai įmanoma įgyvendinti panaudojant elektroninį parašą[126], kurio pagrindas yra viešojo kodavimo rakto infrastruktūra (PKI angl. – *Public Key Infrastructure*) ir abipuse autentifikacija ir šifravimu[127] (apie tai bus kalbama aptariant RFID).

Reglamento 4 straipsnis apima specialias duomenų apsaugos normas. Remiantis minėto straipsnio 1 dalimi „asmenys, kuriems išduodamas pasas [...], turi teisę patikrinti pase [...] įrašytus asmens duomenis ir prireikus prašyti, kad jie būtų ištaisyti ar panaikinti.“ Kadangi pats asmuo

---

[123] 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004, dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:LT:HTML; Prisijungimo laikas 2007-10-12.

[124] Reikia pažymėti, kad remiantis Sutarties dėl Konstitucijos Europai ir ją pakeitusios Lisabonos sutarties III dalies 125 straipsnio 2 dalimi, asmens tapatybės kortelės jau patenka į ES reguliavimo sritį. // http://eur-lex.europa.eu/LexUriServ/site/lt/oj/2004/c_310/c_31020041216lt00410054.pdf; Prisijungimo laikas 2007-10-12

[125] 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004, dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų. // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:LT:HTML; Prisijungimo laikas 2007-10-12, 1 straipsnio 2 dalis.

[126] Integralumas ir autentiškumas.

[127] Konfidencialumas.

negali to padaryti[128], tai pasą išdavusi institucija (ar kita atsakinga institucija) privalo įrengti viešose vietose sistemas, kur žmogus galėtų patikrinti, kokia informacija yra saugoma jo paso RFID luste. 4 straipsnis 2 dalis nustato, kad valstybės pase „nepateikiama jokia mašininio skaitymo informacija, jei ji nenumatyta [...] reglamente ar jo priede, arba jei ji nepaminėta išdavusios valstybės narės pase ar kelionės dokumente, vadovaujantis nacionaliniais teisės aktais.

Remiantis Reglamento 4 straipsnio 3 dalimi biometrinės savybės pasuose „naudojamos tik patikrinti: a) dokumento autentiškumą; b) savininko asmens tapatybę.“ Reikia pažymėti, kad nors ir yra numatytas griežtai apribotas biometrinės informacijos panaudojimas, tačiau Reglamentas palieka valstybėms narėms galimybę nustatyti ir kitus šios informacijos patikrinimo atvejus, kai asmens tapatybės nustatymui „pasą [...] reikalaujama pateikti pagal teisės aktus.“ Taip yra įgyvendinamas skaidrumo principas ir nustatoma draudimas naudoti paso duomenis be duomenų subjekto žinios. Tuo pat metu yra apribojamos perteklinio automatinių biometrinių technologijų naudojimo galimybės, numatant, jog „Pase ar kelionės dokumente nepateikiama jokia mašininio skaitymo informacija, jei ji nenumatyta šiame reglamente ar jo priede, arba jei ji nepaminėta išdavusios valstybės narės pase ar kelionės dokumente, vadovaujantis nacionaliniais teisės aktais“ (4 straipsnio 2 dalis).

### *2. Tarptautinės civilinės aviacijos organizacijos standartai*

Europos Sąjungos ir valstybių narių praktika biometrijos technologijų naudojimo srityje, visų pirma – diegiant biometrinius pasus yra tampriai susijusi su dvejų išorės veikėjų – Jungtinių Amerikos Valstijų ir Tarptautinės civilinės aviacijos organizacijos (TCAO; angl. *Inetrnational Civil Aviation Organization (ICAO)*) teikiamais standartais. Šio proceso iniciatorės – JAV priimto Sustiprintos sienų apsaugos bei įvažiavimo vizų reformos įstatymo[129] 303 straipsnis nustato, kad „ne vėliau kaip 2004 m. spalio 26 d.[130], kad kiekviena numatyta šalis, dalyvausianti JAV vizų atsisakymo programoje[131], [...] turi garantuoti [...], kad įgyvendins programą nustatančią išdavimą automatiškai nuskaitomų pasų, kurie yra apsaugoti nuo padirbinėjimo, su įrašytais biometriniais duomenimis ir [...], atitinkantys nustatytus Tarptautinės civilinės aviacijos organizacijos standartus“.

---

[128] Dėl elektroninės laikmenos ir joje esančių duomenų užšifravimo.
[129] Enhanced Border Security and Visa Entry Reform Act of 2002. // http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf. ; Prisijungimo laikas 2007-10-13.
[130] Šis terminas buvo du kartus pratęstas per vienerius metus, tačiau padarė didelį spaudimą JAV vizų atsisakymo programoje dalyvaujančių šalių valdžioms.
[131] Visa Waiver Program (VWP), US Department of State. // http://travel.state.gov/visa/temp/without/without_1990.html ; Prisijungimo laikas 2007-10-13.

Europos Sąjungos valstybių narių biometriniams dokumentams taikomi minimalūs saugumo standartai numatyti reglamento 2252/2004 priede.[132] Šie reikalavimai yra susieti su TCAO standartais, visų pirma su pagrindiniu standartu reguliuojančiu kelionės dokumentų parametrus – Doc 9303, šiuo metu galiojančiu jo 6 variantu. Pasų standartą nustatančiame 1 dokumento tome išskiriamos dvi dalys: pirmojoje apibrėžiami įprastieji pasai, o antroje su biometrijos integravimu į pasus susiję aspektai. Visų šalių narių prašymu TCAO nusprendė standartizuoti biometrinių duomenų įrašymą į MRTD (angl. *machine readable travel documents*; mašininio nuskaitymo kelionės dokumentai). Standarto kūrimu užsiima TAG/MRTD (*Technical Advisory Group* - MRTD techninių patarėjų grupė). TAG/MRTD išleido technines ataskaitas[133], kurios įtrauktos į pagrindinį Doc 9303 dokumentą. Visos šalys naudoja šias ataskaitas kaip pagrindinį biometrinių duomenų integravimo į kelionės dokumentus standartą.

Nors TACO standartai ir rekomendacijos nėra privalomi, tačiau, kaip buvo minėta anksčiau, Tarybos reglamentas nustatė, kad valstybės narės[134] turi jų laikytis biometrinių pasų atžvilgiu. TCAO priėmė sprendimą, kad veido biometrija yra pagrindinė ir vienintelė privaloma biometrija, kuri turi būti įrašyta į automatinio nuskaitymo kelionės dokumentus. Kiekviena šalis gali nuspręsti kokias papildomas biometrijas įrašyti į kelionės dokumentus. Reglamento Nr. 2252/2004 nuostatos reikalauja, kad į kelionės dokumentus būtų integruojamas bekontaktis lustas, į kurį būtų įrašomi veido ir pirštų antspaudų biometriniai duomenys. Reikia pažymėti, kad pirštų antspaudų nereikalauja nei TCAO, nei JAV, tai yra Europos Sąjungos Tarybos sprendimas.

Kadangi daugelis pasaulio šalių įsipareigojo laikytis TCAO nustatytų rekomendacijų dėl automatiškai nuskaitomų pasų (Doc 9303), ši organizacija gavo viena iš įtakingiausių vaidmenų formuojant biometrijos naudojimo atpažinimui politiką.

Kitą vertus, TCAO patikimumą kvestionuoja faktas bei kritika dėl nedemokratinio organizacijos ir jos sprendimų priėmimo pobūdžio[135]. Formaliai TCAO yra tarptautinė organizacija, kurios kiekviena narė turi balsavimo teisę Asamblėjoje. Asamblėja renka TCAO Tarybą, kurią sudaro 33 narės, renkamos, kad užtikrintų „reikiama atstovavimą; 1) valstybėms, turinčioms didelės įtakos oro susisiekimui: 2) valstybėms, neįtrauktoms kitu pagrindu, bet daugiausiai prisidedančioms tarptautinę civilinę aviaciją aprūpinant oro navigacijos priemonėmis; ir 3) valstybėms, neįtrauktoms kitu pagrindu, bet jų paskyrimas Taryboje užtikrina atstovavimą visiems pagrindiniams pasaulio

[132] Priede nustatytos paso medžiagų, biografinių duomenų lapo, spaudos būdų, apsaugos nuo kopijavimo ir įrašymo būdo reikalavimai.
[133] Šias technines ataskaitas galima rasti TCAO interneto svetainėje adresu http://mrtd.icao.int/
[134] Išskyrus D. Britaniją ir Airiją.
[135] The Policy Laundering Project // http://www.policylaundering.org/keyplayers/ICAO-issues.html; Prisijungimo laikas 2007-10-13.

geografiniams regionams.“[136] Šios formaliai demokratiškos ir į atstovavimą orientuotos organizacijos ambicijos yra ribojamos praktinių TCAO veiklos aspektų: standartizacijos procesas labai priklauso nuo žmogiškųjų ir finansinių narių resursų, o pasiūlymus dėl naujų standartų galinčios parengti ir juos teikiančios narės, visų pirma – JAV, gali daryti įtaką kitų narių atžvilgiu. Šiuo atveju, TCAO standartai gali būti laikomi priimti naudojantis neskaidriomis procedūromis, diktuojant didžiosioms valstybėms. Ta pati nuomonė atsispindi ir Europos Parlamento pranešime (neprivalomas), kuriame teigiama: „ES reglamente nereikia įrašyti nuorodos į Dokumentą Nr. 9303, nes jį galima nuolat keisti pagal procedūrą, kuri nėra nei skaidri, nei demokratiškai pagrįsta.“[137]

Kaip matyti, biometrijos taikymo Europos Sąjungoje politika yra ženkliai įtakojama išorės veiksnių – politinės JAV valios bei tam tikrą įdirbį šioje srityje turėjusios TCAO. Viena vertus, šios aplinkybės turi teigiamą poveikį biometrijos reglamentavimo ir naudojimo praktikos formavimuisi. Šiuos standartus rengiant plačiu tarptautiniu lygmeniu bei naudojantis ekspertinių institucijų pagalba galima pasiekti, jog bus formuojama vieninga, o ne kelios atskiros ir galimai tarpusavyje sunkiai suderinamos politikos. Kitą vertus, techninių biometrija paremtų dokumentų standartų rengimo perdavimas neutraliai ir technokratinių tikslų siekiančiai TCAO gali būti kvestionuojamas dėl praktinių šių taisyklių parengimo aspektų. Atsižvelgiant į šias aplinkybes tikėtina, jog šis biometrijos diegimo būdas bus efektyvesnis nei atskirai formuojami standartai, tačiau dėl ES pareikštų politinių išlygų bet kokių radikalesnių pasiūlymų diegimas tarptautiniu mastu gali būti atmestas.

## *3. Biometrijos naudojimo pasuose sąlygojamos problemos*

ES duomenų apsaugos darbo grupė akcentuoja, jo prieš įvedant pasus su biometriniais duomenimis, yra būtina išsami diskusija visuomenėje dėl šių dokumentų teisinių, etinių ir techninių aspektų. Daugelyje Europos šalių tokia diskusija vyksta ir joje aktyviai dalyvauja valstybės institucijos, nevyriausybinės organizacijos bei biometrinių duomenų naudojimo pasekmėms analizuoti įsteigtų institucijų ekspertai. Daugiausia klausimų kyla dėl planuojamo biometrinių duomenų saugojimo registruose (duomenų bazėse), biometrinių duomenų naudojimo tikslingumo, klaidingo atpažinimo (patvirtinimo) procedūros, radijo dažnio identifikavimo (RFID) technologijos

[136] 1944 m. gruodžio 7 d. Tarptautinė civilinės aviacijos konvencijos (Čikagos konvencijos) 50 straipsnio b) dalis // http://www.caa.lt/admin/files/get.php?id=303 ; Prisijungimo laikas 2007-10-13.

[137] Komisijos pasiūlymas dėl Tarybos reglamento dėl Europos Sąjungos piliečių pasų apsaugos savybių ir biometrinių duomenų standartų [15139/2004 - 15139/2004 - 2004/0039(CNS)] // http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2004-0028&language=LT&mode=XML#title1 ; Prisijungimo laikas 2007-10-13.

naudojimo pasuose. Šioje darbo dalyje nagrinėsime minėtas problemas remdamasis Europos Sąjungos narių, tame tarpe ir Lietuvos pavyzdžiais.

## 3. 1. Nacionalinių duomenų bazių steigimo klausimas: Vokietijos ir D.Britanijos atvejai

Priimant sprendimą asmens tapatybės dokumentuose taikant biometrines technologijas kyla klausimas dėl biometrinių asmens duomenų saugyklų. Europos Sąjungos teisėje šį klausimą reglamentuojančiame reglamente EB 2252/2004 „Dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų“ funkcija yra palikta valstybėms narėms. Techniškai į šį klausimą galimi du atsakymo variantai – asmens duomenis saugoti centralizuotai – nacionalinėje centrinėje duomenų bazėje arba juos laikyti periferinėse duomenų talpyklose, paprastai pačiuose asmens identifikavimo dokumentuose. Tarpinis variantas – nedidelio mąsto centralizuotų duomenų bazių steigimas yra taikomas tik sąlyginai nedidelės ir uždaros asmenų grupės atveju (pvz. įmonės darbuotojų, turinčių prieigos prie tam tikro objekto teisę).

Centralizuotą nacionalinių biometrinių duomenų bazių kūrimo būdą paprastai renkasi valstybės, siekdamos užkirsti kelią piliečiams susikurti daugiau nei vieną tapatybę įsigijus keletą pasų skirtinga pavarde bei užsitikrinti operatyvaus visapusiško asmens tapatybės patikrinimo galimybę. Ši problema ypač aktuali tuo atveju, jei šalyje neveikia bendras nuolatinių gyventojų registras arba jis kuriamas tuo pačiu metu, kai įvedami nauji tapatybės dokumentai. Tolimesnėje darbo dalyje analizuojama skirtingus šios klausimo sprendimo būdus pasirinkusių dvejų didžiųjų ES valstybių narių – D.Britanijos ir Vokietijos pasirinkta metodika, kartu aptariant ir Lietuvoje taikomas priemones.

Didžiojoje Britanijoje 2006 m. Tapatybės kortelių įstatymu[138] numatyta, kad kiekvienas nuolatinis gyventojas sulaukęs „16 metų amžiaus“[139] gaudamas tapatybę patvirtinantį dokumentą (tapatybės kortelę arba pasą) bus įtrauktas Nacionalinį tapatybės registrą. Šiuo metu Britanijoje jau veikia keletas valstybinių duomenų bazių (registrų), kuriuose saugomi duomenys apie gyventojus, tačiau minėto Nacionalinės tapatybės registro, kuriuo „siekiama nustatyti naują „aukso standartą

[138] Identity Cards Act 2006 (c. 15) // http://www.legislation.gov.uk/acts/acts2006/20060015.htm; Prisijungimo laikas: 2007-11-03.
[139] Identity Cards Act 2006 (c. 15) // http://www.legislation.gov.uk/acts/acts2006/20060015.htm; Prisijungimo laikas: 2007-11-03, 2 (2) a straipsnis.

viešajam ir privačiam sektoriui“[140], esminis skirtumas tas, kad bus saugomi biometriniai duomenys (visų 10 pirštų antspaudai, skaitmeninis veido, akies rainelės atvaizdas) ir jie bus susieti su kitais asmenį identifikuojančiais duomenimis, tokias kaip asmens vardas, namų adresas ir kt.[141]

Lietuvoje taip pat buvo priimta sprendimas biometrinius duomenis (skaitmeninis veido atvaizdas ir pirštų antspaudai[142]) pradėti saugoti registre, tik šiuo atveju nereikėjo kurti naujos duomenų bazės; tam buvo pritaikyta jau veikianti Gyventojų registro infrastuktūra. Kaip jau minėta, 2006 metų Paso, Tarnybinio paso, Gyventojų registro įstatymų pakeitimo ir papildymo įstatymais, buvo nustatytas pasuose įrašytų biometrinių duomenų (skaitmeninių veido atvaizdų bei pirštų antspaudų) naudojimas, kaupimas bei saugojimas Gyventojų registre.

Tuo tarpu Vokietijos įstatymai nacionalinės duomenų bazės sukūrimo galimybę eliminavo 2002 m. Paso įstatymu[143]. Dar daugiau – konstituciniai reikalavimai Vokietijoje yra griežtesni nei daugelyje kitų valstybių. Tai reiškia, kad bendra centrinė duomenų bazė (ir decentralizuoti jos atitikmenys) būtų nesuderinama su „teisė apsispręsti dėl informacijos“[144], kuri yra sudėtinė pagrindinių teisių, numatytų Vokietijos konstitucijoje, dalis. Naujieji Vokietijos Nacionalinio paso įstatymo pakeitimai taip pat nenumato ir pirštų antspaudų saugojimo pasų išdavimo institucijų duomenų bazėse galimybės. Pagaminus pasą, gamintojas ir pasus išduodančios įstaigos privalo sunaikinti duomenis. Be to, tai turi būti padaryta po kiekvieno patikros proceso. Be trumpalaikio duomenų apdorojimo specifinėse patikrinimo situacijose pirštų atspaudai yra saugomi tik pačiame Vokietijos piliečio pase ir jokiose kitose viešosios valdžios duomenų bazėse.

Kaip matyti, didžiausios ES valstybės narės – Vokietija ir D.Britanija pasirinko skirtingas biometrinių duomenų saugojimo metodikas. D. Britanijos pasirinktas modelis centrinės valdžios institucijoms užtikrina efektyvesnes gyventojų kontrolės galimybes, tačiau kartu sąlygoja ir papildomų problemų dėl centralizuotai saugomų duomenų saugumo ir pačios metodikos suderinamumo su biometrijos ekspertų rekomendacijomis. Pastaruoju aspektu pažymėtinas britiško požiūrio neatitikimas su Direktyvos 29 straipsnio Duomenų apsaugos darbo grupės nuomone[145],

---

[140] Sullivan, Clare The United Kingdom *Identity Cards Act 2006* – proving Identity?, *MqJBL (2006) Vol 3*, p. 259, http://www.law.mq.edu.au/html/MqJBL/vol3/12Sullivan.pdf; Prisijungimo laikas: 2007-11-03.

[141] Home Office.Strategic Action Plan for the National Identity Scheme: Safeguarding your identity. Gruodis, 2006 // http://www.ips.gov.uk/passport/downloads/Strategic_Action_Plan.pdf; Prisijungimo laikas: 2007-11-03.

[142] Pažymėtina, kad Lietuvos Respublikos Vyriausybės 2007 m. nutarimu Nr. 318 „Dėl Lietuvos Respublikos gyventojų registro nuostatų patvirtinimo“ nustatoma gyventojų registro nuostatų normos dėl Lietuvos Respublikos piliečių pirštų atspaudų tvarkymo įsigalioja nuo pirštų atspaudų įrašymo elektroniniu būdu Lietuvos Respublikos pasuose ir tarnybiniuose pasuose pradžios.

[143] 4 (4) straipsnis. Paßgesetz, 1986. // http://www.aufenthaltstitel.de/passg.html; Prisijungimo laikas: 2007-10-26.

[144] Angl. *Informational self-determination* // http://en.wikipedia.org/wiki/Informational_Self-Determination.

[145] Direktyvos 95/46/EB 29 str. Darbo grupės 2005 m. rugsėjo 30 d. Nuomonė Nr. 1710/01, WP 112 „Dėl 2004 m. gruodžio 13 d. Tarybos reglamento (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų įgyvendinimo (Nuomonė 2005/3)“// ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_lt.pdf; Prisijungimo laikas: 2007-08-29.

kuria ji yra išsakiusi savo nepritarimą tokiam duomenų kaupimui, akcentuodama kad „bet kuri centrinė duomenų bazė padidintų neteisėto duomenų panaudojimo ir pasisavinimo pavojų. Ji taip pat padidintų piktnaudžiavimo ir funkcijos deformacijos riziką“ – taip gali būti pažeidžiamas proporcingumo principas. Savo ruožtu Vokietijos vyriausybė ir Bundestagas, griežtai laikydamiesi nacionalinių konstitucinių reikalavimų bei minimalaus duomenų kiekio saugojimo principo, atsisakė galimybės kartu su naujo pavyzdžio pasų įdiegimu sukurti ir centrinę biometrinių duomenų bazę. Šiuo atveju asmens duomenų saugumas užtikrinamas didinant pačių pasų, kaip informacijos kaupyklų, saugumą. Savo ruožtu skirtumus tarp britiškos bei vokiškos biometrinių duomenų saugojimo metodikos galima aiškinti dvejų veiksnių kombinacija – duomenų valdymo efektyvumas skatina rinktis centralizuotą biometrinių duomenų saugojimą, tuo tarpu nacionaliniai teisiniai apribojimai – periferinį.

## 3. 2. Biometrinių duomenų taikymo tikslingumas

Kaip buvo minėta anksčiau, biometrinių duomenų naudojimas yra ribojamas ES reglamentu, tačiau šis teisės aktas palieka valstybėms narėms galimybę nustatyti ir kitus šios informacijos patikrinimo atvejus. Taigi keliamas svarbus klausimas, kokius papildomus tikslus valstybės narės laiko tinkamais ir ar šie tikslai atitinka tam tikrus konstitucinius reikalavimus.

Tyrinėtojai pažymi, jog biometriją galima apibrėžti kaip vieną iš trijų asmens identifikavimo priemonių, greta atitinkamo ženklo turėjimo (paso, kortelės, dokumento) bei pažinimo (slaptažodžio žinojimo).[146] Toks apibrėžimas palieka dideles galimybes biometrijos naudojimo tikslingumo interpretacijai.

Nepaisant gana plataus biometrijos apibrėžimo, didžiausios ES valstybės narės – Vokietijos Paso įstatymas nenumato kitų tikslų, išskyrus tuos, kurie nurodyti reglamente, reguliuojančiame pasų duomenis. Šiuo įstatymu suteikiami įgaliojimai atitinkamoms policijos, muitinės, pasų registracijos įstaigoms, tačiau Paso įstatymo 16 straipsnio 6 punktas aiškiai nustato, kad biometrinių duomenų naudojimas apsiriboja dokumento ir jį pateikusio asmens autentiškumo nustatymu (patikrinimu). Kitoms įstaigoms, taip pat ir privatiems asmenims naudoti biometrinius duomenis yra griežtai draudžiama.

Policijos įstaigos kaip ir anksčiau gali naudoti veido duomenis vykdydamos baudžiamąjį persekiojimą. Kaip jau minėta, Vokietijos Paso įstatymas aiškiai užkerta kelią centrinės duomenų

[146] Guerrier C., Cornelie L-A, Les aspects juridiques de la biometrie, http://www.biometrie-online.net/dossiers/generalites/droit/Claudine%20GUERRIER.pdf ; p. 1, Prisijungimo laikas: 2007-10-26.

bazės sukūrimui, taip pat neleidžiama ieškoti konkretaus veido duomenų (pvz., per CCTV kamerą). Be to, atrodo, kad techniškai neįmanoma per protingą terminą identifikuoti veidą biometrinėje duomenų sistemoje, turinčioje 70 milijonų įrašų su priimtinu klaidos laipsniu. Kito pagrindinio biometrinio požymio - pirštų atspaudai nėra saugomi jokiose duomenų bazėse, todėl šiuo atžvilgiu nekyla jokių duomenų apsaugos klausimų.

D.Britanijos teisėje, numatančioje centrinės biometrinių duomenų bazės sukūrimą, taip pat yra ribojamos biometrijos taikymo galimybės, numatant tris atvejus:

- tapatybės autentifikavimą registracijos metu;
- tapatybės verifikavimą atsakant numatytų viešųjų ar privačių organizacijų užklausą;
- asmens tapatybės nustatymą pagal Nacionaliniame tapatybės registre užfiksuotus duomenis (pvz. nusikaltimo vietoje paimtus pirštų antspaudus)[147]

Kartu C.Sullivan pažymi esminį D.Britanijos modelio trūkumą – biometrinių duomenų savininkas yra lyginamas su duomenimis tik jų duomenų registravimo metu: nors paprastai duomenų savininko dalyvavimas registravimo metu bus laikomas įprastine praktika, tačiau galimos ir išimtys.[148] Visos kitos Nacionalinio tapatybės registro paslaugos yra teikiamos lyginant pateiktą informaciją su saugoma duomenų bazėje (be duomenų savininko dalyvavimo).

Kaip matoma, D. Britanijoje įdiegtas modelis užtikrina labai dideles asmens identifikavimo galimybes, tiek verifikuojant jo deklaruojamą tapatybę (sutikrinant su centrinės duomenų bazės duomenimis), tiek ir nustatant tam tikrų biometrinių duomenų savininką. Ši teisė yra suteikiama ir valstybiniams ir privatiems subjektams, įtrauktiems į nacionaliniu mastu sudaromą tokių asmenų sąrašą. Įstatymas riboja biometrinių duomenų gavimo galimybes, nurodydamas, jog jie gali būti tiekiami tik lyginant pareiškėjo jau turimus duomenis su saugomais Nacionaliniame tapatybės registre, o pats tapatybės identifikavimas yra apibrėžiamas kaip „asmens tapatybės nustatymas, viršijant pagrįstas abejones“,[149] t.y. duomenis tikrinantis subjektas turi pagrįsti tikrinimo reikalingumą.

Lietuvos atveju, taip pat naudojant centralizuotą biometrinių duomenų bazę, biometrinių duomenų naudojimo atvejai yra apibrėžti labai trumpai. Biometrinių duomenų kaipimą reglamentuojančiame Gyventojų duomenų registro įstatyme yra tik nurodomi kaupiami duomenys (asmens kodas, vardas (vardai), pavardė (pavardės), lytis, gimimo data, pilietybė (pilietybės),

---

[147] Sullivan, Clare The United Kingdom *Identity Cards Act 2006* – proving Identity?, *MqJBL (2006) Vol 3,* p. 259, http://www.law.mq.edu.au/html/MqJBL/vol3/12Sullivan.pdf; Prisijungimo laikas: 2007-11-03.

[148] Teisės akto 5(5) straipsnyje numatoma, jog „*gali būti* reikalaujama, jog asmuo [...] dalyvautų, [...] pats pateiktų [...] biometrinę informaciją, Identity Cards Act 2006 // http://www.legislation.gov.uk/acts/acts2006/20060015.htm; Prisijungimo laikas: 2007-11-03.

[149] British Broadcasting Commission, *Q&A Identity Card Plans*, 30 March 2006, http//:www.newsvote.bbc.co.uk.html, 3 April 2006. Prisijungimo laikas: 2007-10-26.

gimimo vieta, gyvenamoji vieta, šeiminė padėtis ir jos pasikeitimo data, mirties data, tėvų, vaikų ir sutuoktinių asmens kodai, tautybė, veido atvaizdas, pirštų atspaudai, parašas).[150] Kartu numatoma, jog biometriniai duomenys (veido atvaizdas, pirštų atspaudai, parašas) gali būti teikiami tik teisėtvarkos bei asmens tapatybę patvirtinančius dokumentus išduodančioms institucijoms.[151]

Kaip matyti iš pasirinktų trijų reglamentavimo atvejų analizės, Lietuva pasirinko tam tikrą tarpinį modelį tarp labai griežto, centralizuoto duomenų kaupimo atsisakiusios Vokietijos bei gan liberalaus, centralizuotą duomenų bazę kuriančios ir keletą duomenų teikimo galimybių numačiusios D.Britanijos varianto. Pagal įstatyme nurodytas teisę gauti saugumus biometrinius duomenis turinčias institucijas galiam teigti, jog Lietuvos Gyventojų registre kaupiami biometriniai duomenys yra skirti tik gyventojų tapatybės dokumentų išdavimo ir kovos su nusikalstamumu tikslais, jų naudojimas kitiems tikslams, pvz. socialinių išmokų gavėjų kontrolei nėra numatomas.

## 3. 3. Atsarginės procedūros

Kiekviena biometrinė sistema susiduria su problema, kai dėl tam įvairių priežasčių tam tikra populiacijos dalis laikinai arba nuolat negali pateikti biometrinių požymių. Be to, dauguma neatpažinimo atvejų įvyksta atmetant duomenis tiesiog dėl klaidos. Netgi esant santykinai žemam klaidingo atmetimo laipsniui, tokių klaidingų atmetimo atvejų bus labai daug: pvz. Frankfurto prie Maino oro uoste sistemoje, kurios klaidingo atmetimo laipsnis yra 1 %, gali pasitaikyti daugiau nei 1000 klaidingų pavojaus signalų per dieną.

Šiuo metu nėra aišku, kiek žmonių iš tikrųjų susidurs su šiomis problemomis. Tačiau aišku, kad valstybės turės įdiegti atsargines procedūras, skirtas tiek užtikrinti saugų visų asmenų identifikavimą, tiek išvengti tų, kurie negali užsiregistruoti sistemoje, diskriminacijos. Kadangi vienodo elgesio principas yra visų konstitucinių sistemų, taip pat ir Europos žmogaus teisių konvencijos dalis (14 str.), jis taikomas visoms valstybėms narėms. Todėl kontrolės punktuose bus neįmanoma pasikliauti vien tik biometriniu identifikavimu. Be to, atsarginės procedūros turi būti pajėgios užkirsti kelią vilkinimams.

Tai, ar šis reikalavimas sukels sienos apsaugos tarnyboms didelių problemų, ar ne, taps aišku, kai pasų sistema pradės normaliai veikti, nes faktinės pasekmės pasų turėtojams priklauso nuo tolesnio proceso (leidimo pakartotiniam atpažinimui, nuodugnių kontrolės procedūrų ir t.t.). Tai taip pat taikoma tiems pasų turėtojams, kurių pirštų atspaudai dėl įvairių priežasčių yra mažai tinkami

[150] Lietuvos Respublikos Gyventojų registro įstatymas, 9 straipsnis // Valstybės žinios. 1999, Nr. 28-793.
[151] Ten pat.

biometriniam atpažinimui. Šie asmenys gali patirti papildomų sunkumų dėl žymiai aukštesnio individualaus klaidingo atmetimo laipsnio nei vidutinis vartotojas. Siekiant išvengti tokių nepatogumų, kontroliuojančiam asmeniui būtų pravartu turėti galimybę pasinaudoti oficialiai patvirtinta informacija apie tokius atvejus.

Vienas sėkmingų šios problemos pavyzdžių yra Vokietijos Paso įstatymas, kurio 4 (3) skyriuje numatomas informacijos saugojimas biometrinių duomenų pavidalu tik paso luste.

Bet kuriuo atveju tapatybės dokumento pagrindinė dalis turi būti apsaugota nuo suklastojimo ir įmanoma naudoti be lusto, nes ji gali būti sunaikinta jos savininkui to nežinant. Tuo pačiu metu yra labai sudėtinga leisti „visuotinai“ naudoti pasus su sunaikintais lustais, kadangi tai gali sudaryti sąlygas išvengti biometrinės kontrolės ir kartu sukelti abejones dėl viso projekto. Atsižvelgiant į šią problematiką yra numatoma galimybė, jog asmens tapatybė bus tikrinama ne vien biometrinėmis technologijomis, tačiau ir naudojant įprastines priemones.

## 3. 4. Neautorizuoto duomenų nuskaitymo problema

Vienas esminių sunkumų, su kuriais susiduria bet kokios asmens duomenis naudojančios sistemos, yra juose saugomų biometrinių duomenų saugumo užtikrinimas, apsauga nuo neautorizuoto jų nuskaitymo. Ši problema tampa labai aktualia ne tik identifikavimo dokumento vagystės atveju, tačiau ir taikant bekontakčio / nuotolinio tapatybės nustatymo technologijas.

Jau aptartoje TCAO parengtoje biometrinių duomenų įtraukimo į kelionės dokumentų rengimą numatytas nuotolinio veikimo lustų naudojimas pasižymi ilgaamžiškumu, tačiau neišsprendžia neautorizuoto duomenų nuskaitymo problemos. Dėl nuotolinio duomenų nuskaitymo galimybės negalima garantuoti, jog duomenys, saugomi tokiuose lustuose, nebus nuskaitomi apie tai nežinant kortelės turėtojui („paviršutiniško perskaitymo“ problema). Be to, įmanoma įsiterpti į ryšio seansą tarp lusto ir skaitytuvo („slaptas pasiklausymas“). Taip pat egzistuoja neteisėto naudojimo problemos kortelės praradimo ar vagystės atveju.

Iš pradžių TCAO nenumatė jokių saugumo priemonių (tokių kaip tapatumo nustatymas ir/arba užšifravimas). Tai būtų palikę kortelės turėtojams vienintelę galimybę apsisaugoti, pvz., laikyti pasą metaliniame gaubte (pvz., aliuminio folijoje), nes tai užkirstų kelią radijo dažnio skaitytuvams nuskaityti duomenis.[152]

[152] Atsižvelgiant į biometrinių sistemų sudėtingumą, tokie saugikliai iš pradžių gali pasirodyti šiek tiek absurdiški, tačiau jie pasitvirtino kaip patys efektyviausi privačių duomenų apsaugos įrankiai.

ES Reglamento 1 (2) str. įpareigoja valstybes nares įgyvendinti priemones, kuriomis būtų užtikrinamas duomenų vientisumas, autentiškumas ir konfidencialumas TCAO standartai šiuo metu numato neprivalomas apsaugos priemones. Siekiant įvykdyti šį įpareigojimą, pirmoji biometrinių pasų karta naudoja taip vadinamą „pradinės prieigos kontrolės“ sistemą (PPK). Elektroniniai duomenys (biometriniai požymiai ir kita asmeninė informacija) yra užšifruojami individualiu kodu, kuris priklauso nuo paso dalies, nuskaitomos aparatais, savybių. Kontrolės punktuose ši informacija turi būti nuskaitoma pirmiausia tam, kad atrakintų lustą skaitymui. Taigi kontroliuojantys asmenys privalo nuskanuoti atspausdintas duomenų eilutes tam, kad galėtų nuskaityti lusto duomenis.

Vis dėlto tik spausdintais duomenimis paremtas PPK saugumas yra diskutuotinas, kadangi paso dalies, nuskaitomos aparatais, savybės yra prieinamos kiekvienam, kuris turi pasą. Savo ruožtu PPK sistema neapsaugo nei praradimo ar vagystės atveju, nei nuo tų, kas teisėtai ar neteisėtai įgyja duomenis apie paso dalį, nuskaitomą aparatais. Dėl šios priežasties antroji pasų karta (su pirštų atspaudų duomenimis) bus aprūpinta „išplėstine prieigos kontrolės“ sistema (IPK), kuri remiasi automatiniu abipusiu lusto ir skaitytuvo atpažinimu. Šioje PKI infrastruktūroje kiekviena šalis įkurs Šalies atestato patvirtinimo įstaigą (ŠAPĮ), kurios atestatai bus saugomi tos šalies pasų lustuose. ŠAPĮ išduos atestatus Dokumentų tikrintojams kitose šalyse, kurie, savo ruožtu, administruos savo skaitytuvų atestatus. Ši sistema leidžia riboti duomenų perdavimą iš paso lusto į skaitytuvus, turinčius atestatus, kurie gali būti atsekti iki atestatą išdavusios ŠAPĮ. Atitinkamai kiekviena šalis gali spręsti, kuriai kitai šaliai suteikti prieigą prie duomenų. IPK schema sumažina biometrinių pasų duomenų apsaugos problemas, tačiau išlieka tokie sunkumai kaip pavogtų kortelių skaitytuvai su galiojančiais atestatais, taip pat tai, kad lustas nesaugo duomenų apie laiką ir neturi prieigos prie patikimo laiko šaltinio, tuo apsunkindamas kortelės skaitytuvo atestato galiojimo laiko patikrinimą.

Kaip matyti iš praktinės biometrinių duomenų taikymo apžvalgos, nepaisant sparčios biometrijos plėtros, lieka nemaža techninių su šia technologija susijusių problemų. Vienas pagrindini(ų klausimų, į kuriuos daugelis valstybių pateikia skirtingus atsakymus, yra biometrijos naudojimo ribos: kokiais atvejais ir kas turi turėti teisę reikalauti pateikti biometrinius duomenis ir naudoti. Aptarti trys biometrijos naudojimo reglamentavimo atvejai rodo, tris skirtingas tendencijas – vien tik asmens privatumo argumentais paremtas požiūris (Vokietija) numato biometrijos taikymo galimybes tik verifikuojant identifikavimo dokumento savininko tapatybę, tarpinis (Lietuvos) pasirinktas modelis, numatantis centralizuotos duomenų bazės naudojimą, jos funkcijas apriboja tik tapatybės nustatymo ir kovos su nusikalstamumu tikslais, tuo tarpu valstybės interesus akcentuojantis D.Britanijos modelis lanksčiai numato galimybę biometrinius duomenis naudoti visoms į atskirą sąrašą įtrauktoms valstybinėms ir privačioms institucijoms. Nepaisant to, ši

technologija yra diegiama visų pirma įgyvendinant griežtus duomenų saugumo standartus bei papildomo patikrinimo galimybes.

Kitos dvi esminės biometrijos naudojimo sąlygojamos problemos – duomenų sauga ir papildomos kontrolės priemonių poreikis dėl savo labiau techninio pobūdžio sąlygoja mažesnę sprendimo būdų įvairovę. Iš esmės yra sutinkama, jog yra būtina stiprinti biometrijoje naudojamų asmens duomenų saugos priemones, tiek esančių centralizuotose, tiek ir periferinėse duomenų bazėse, taip pat tobulinti nuotolinio nuskaitymo technologijas. Taip pat pažymėtina, jog praktinis biometrinių duomenų naudojimas apima papildomos kontrolės priemones – bet kuriuo atveju tapatybę tikrinantis asmuo turi lyginti identifikavimo dokumente nurodytas asmens savybes su jų valdytojo duomenimis, o esant centralizuotai duomenų bazei – ir su jos pateikta informacija. Be to, atsižvelgiant į technologinius aspektus yra numatoma biometrinės patikros rezultatų kvestionavimo galimybė – t.y. asmens teisė reikalauti, jog jo tapatybė būtų tikrinama ir tradicinėmis priemonėmis.

# Išvados

Iš atlikto darbo galima padaryti šias išvadas:

1. Asmens identifikavimui naudojamų technologijų raida bei platus biometrinių duomenų naudojimas XX a. pabaigoje sąlygojo diskusijos dėl teisinio biometrijos naudojimo ir biometrinių duomenų kaupimo reglamentavimo atsiradimą. Tarptautiniai susitarimai dėl biometrinių duomenų, pradedant devintojo dešimtmečio Europos Tarybos ir Ekonominio bendradarbiavimo ir plėtros organizacijos dokumentais, pabrėžią jų ypatingumą bei poreikį atsižvelgti į žmogaus teisų, visų pirma - teisės į privatumą, reikalavimus.

2. Direktyva kartu su Europos Tarybos 1981 m. Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis ir 1980 m. EBPO Asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairėmis nustato teisinį biometrinių technologijų Europoje pagrindą.

3. Biometrinių duomenų rinkimas, saugojimas ir naudojimas kelia esminius klausimus dėl šių veiksmų suderinamumo su žmogaus teisių ir ypač – teisės į privatumą, apsaugos standartais. Šios abejonės yra susiję su dvejais pagrindiniais klausimų rinkiniais – asmens duomenų apsauga nuo neteisėto pasinaudojimo ir naudojamų biometrinių technologijų tikslumas.

3.1. Atsakant į abejones dėl asmens duomenų apsaugos, biometrija paremtų technologijų naudojimas yra sąlygojamas keleto pamatinių, nuo devintojo dešimtmečio pradžios akcentuojamų reikalavimų: duomenų rinkimo apribojimo, duomenų kokybės, duomenų rinkimo tikslingumo, duomenų naudojimo apribojimo, saugumo užtikrinimo, atvirumo, individualaus dalyvavimo bei duomenų valdytojo atskaitomybės principų.

4.2. Biometrinių asmens duomenų rinkimo galimybė yra teisiškai apribota sąlyga turėti nedviprasmišką duomenų subjekto sutikimą, būti įvykdžius duomenų tvarkytojui tenkančią prievolę informuoti duomenų subjektą apie duomenų kaupimo tikslą, vykdomą užduotį kartu pripažįstant, jog duomenų subjekto teisės ir laisvės yra viršesnės nei duomenų rinkimo tikslai.

4.3. Biometrinių duomenų kaupimo klausimas kvestionuoja individų teisę į privatumą bei kelia abejones dėl jų saugyklų patikimumo neteisėto panaudojimo atžvilgiu. Ši problema sprendžiama įgyvendinant duomenų kaupimo pagrįstumo principą, saugant mažiausius reikalingus jų kiekius bei trumpiausią pagrįstą laiką; taip pat siūloma nediegti centralizuotų duomenų bazių, naudoti periferines asmenį identifikuojančias priemones su biometriniais duomenimis.

4.4. Biometrinių technologijų tikslumas išlieka pilnai neišspręstu klausimu, net ir šios srities ekspertams pripažįstant, jog neįmanoma garantuoti visiško tikslumo: tiek dėl technologinių

priežasčių, tiek ir dėl to, jog kai kurie biometriniai asmenų duomenys, pvz. veido forma, balso tembras ir kt. su amžiumi kinta. Kaip vienintelė galima kompensacinė priemonė yra siūlomas dubliuojančių technologijų taikymas, asmens tapatybės patvirtinimui.

5. Vienas svarbiausių su biometrija susijusių klausimų yra šios technologijos naudojimo apimtis. atskiros valstybės pateikia skirtingus atsakymus į šį klausimą - pvz. Vokietija griežtai riboja biometrinių technologijų taikymą, šia teisę suteikdama tik valstybinėms institucijoms. Kai kurios kitos valstybės - pvz. D.Britanija šią teisę suteikia ir privatiems subjektams. Biometrinių duomenų valdytojo teisinis statusas kol kas nėra sukėlęs esminių teisinių ar politinių kolizijų, tačiau tikėtina, jog ateityje, plėtojantis biometrijos taikymui, šis klausimas gali tapti labai aktualiu.

Atsižvelgiant į darbe aptartą biometrijos problematiką, galima pateikti keletą pagrindinių rekomendacijų, kurias įgyvendinus būtų išspręsta dalis dabartinių skirtingų požiūrių į biometriją šalininkų ginčų.

Pirma, bent Europos Sąjungos (kaip privalomą galią turinčios valstybėms narėms organizacijos), o taip pat – TCAO (kaip saugumo standartus tam tikroje srityje nustatančios organizacijos) lygmeniu įvesti vieningą biometrijos naudojimą reglamentuojančią terminologiją, pateikiant vieningus sąvokų apibrėžimus. Vieningo sąvokų ir apibrėžimų rinkinio parengimas Europos Sąjungos mastu suformuotų politiškai svarų pavyzdį bei modelį, kuriuo galėtų sekti ir trečiosios šalys, formuodamos savo biometrijos naudojimo politiką.

Antra, laikantis minimalaus reikalingo biometrinių duomenų kaupimo ir naudojimo principo bei atsižvelgiant į tai, jog dalis fizinių žmogaus savybių, kuriomis remiantis formuojami biometriniai duomenys bėgant laikui kinta, apsiriboti tik minimaliu būtinu biometrinių žmogaus požymių rinkiniu, kurie normaliomis sąlygomis išlieka pastovūs visą gyvenimą (akies rainelė, piršto antspaudai, kritiniais atvejais - DNR).

Trečia, siekiant maksimaliai apsaugoti biometrijoje naudojamus asmens duomenis, būtina naudoti vietines biometrinių duomenų saugojimo priemones (asmenines korteles), kiek galima labiau vengiant centralizuotų bei nuotoliniu ryšiu pasiekiamų duomenų bazių kūrimo, naudoti ne identifikavimo, o autentifikavimo funkciją. Dėl šių priežasčių, net ir pasirinkus centralizuotos duomenų bazės kūrimo modelį, siūlytina maksimaliai apriboti biometrines technologijas naudoti turinčių teisę institucijų ratą.

Ketvirta, atsižvelgiant į klaidų bei techninių gedimų tikimybę, kartu su biometrinėmis technologijomis būtina kartu įdiegti ir atsargines procedūras, kurių pagalba galima užtikrinti sėkmingą naudojamos technologijos veikimą net ir ekstremaliomis sąlygomis.

Penkta, atsižvelgiant į biometrinių duomenų ypatingą svarbą bei tarptautiniu lygmeniu priimtus susitarimus, prieš pasirenkant taikyti biometrines technologijas, yra svarbu apsvarstyti galimas alternatyvas.

## LITERATŪROS SĄRAŠAS

## TEISĖS AKTAI IR KITI DOKUMENTAI


1. Lietuvos Respublikos Konstitucija // Valstybės žinios. 1992, Nr. 33-1014.
2. Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 2003, Nr. 15-597.
3. Lietuvos Respublikos Elektroninių ryšių įstatymas//Valstybės žinios. 2004, Nr. 69-2382.
4. Lietuvos Respublikos Paso įstatymas // Valstybės žinios. 2001, Nr. 99-3524.
5. Lietuvos Respublikos Tarnybinio paso įstatymas//Valstybės žinios. 2000, Nr. 7-178.
6. Gyventojų registro įstatymas// Valstybės žinios. 1999, Nr. 28-793. Prisijungimo laikas: 2007-11-15.
7. 1944 m. gruodžio 7 d. Tarptautinė civilinės aviacijos konvencija (Čikagos konvencija), http://www.caa.lt/admin/files/get.php?id=303 Prisijungimo laikas: 2007-11-15.
8. 1948 m. gruodžio 10 d. Jungtinių Tautų Organizacijos Visuotinė žmogaus teisių deklaracija // http://www.lexilogos.com/declaration/lituanien.htm; Prisijungimo laikas: 2007-11-15.
9. 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // http://www3.lrs.lt/cgi-bin/preps2?Condition1=114048&Condition2=; Prisijungimo laikas: 2007-10-18.
10. 1980 m. rugsėjo 23 d. EBPO Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių. // http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html; Prisijungimo laikas: 2007-11-15.
11. 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) //Valstybės žinios. 2001, Nr. 32-1059.
12. 1992 m. vasario 7 d. Europos Sąjungos Sutartis (Mastrichto sutartis) // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=32156; Prisijungimo laikas: 2007-11-15.
13. 2000 m. gruodžio 7 d. Europos Sąjungos Pagrindinių teisių Chartija http://eur-lex.europa.eu/LexUriServ/site/lt/oj/2004/c_310/c_31020041216lt00410054.pdf; Prisijungimo laikas: 2007-11-15.
14. 1944 m. gruodžio 7 d. Tarptautinė civilinės aviacijos konvencijos (Čikagos konvencija) // http://www.caa.lt/admin/files/get.php?id=303 ; Prisijungimo laikas 2007-10-13

15. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl 1995 asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // http://eur-lex.europa.eu/Result.do?T1=V3&T2=1995&T3=46&RechType=RECH_naturel&Submit=Ie%C5%A1koti; Prisijungimo laikas: 2007-09-14.
16. 2002 Europos Parlamento ir Tarybos direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“ // http://eur-lex.europa.eu/Result.do?T1=V3&T2=2002&T3=58&RechType=RECH_naturel&Submit=Ie%C5%A1koti, Prisijungimo laikas: 2007-10-15
17. 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 “Dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo” // http://eur-lex.europa.eu/EUDOROrder.do?id_pub=2007/305&volume=1&vl=LT&series=JOL&page_first=64&page_last=64; Prisijungimo laikas: 2007-11-15.
18. 2004 m. gruodžio 13 d. Tarybos reglamentas (EB) Nr. 2252/2004, dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:LT:HTML; Prisijungimo laikas 2007-10-12.
19. 2006 m. birželio 28 d. Komisijos sprendimas K(2006) 2909 nustatantis valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų technines specifikacijas, http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_lt.pdf; Prisijungimo laikas: 2007-11-04.
20. Direktyvos 95/46/EB 29 str. darbo grupės 2001 m. rugsėjo 13 d. Darbinis dokumentas Nr. 12168/02, WP 80 „Dėl biometrinių duomenų“// http://www.ada.lt/images/cms/File/WP80.pdf; Prisijungimo laikas: 2007-08-29.
21. Direktyvos 95/46/EB 29 str. darbo grupės 2002 m. lapkričio 25 d. darbinis dokumentas Nr. 11750/02, WP 67 „Dėl asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis“// http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm ; Prisijungimo laikas: 2007-08-29.
22. Direktyvos 95/46/EB 29 str. darbo grupės 2003 m. rugpjūčio 1 d. darbinis dokumentas (EN) Nr. 12168/02 „Darbinis dokumentas dėl biometrinių duomenų“, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm ; Prisijungimo laikas: 2007-08-29.

23. Direktyvos 95/46/EB 29 str. darbo grupės 2004 m. vasario 11 d. nuomonė Nr. 11750/02, WP 89 „Dėl asmens duomenų tvarkymo vaizdo stebėjimo priemonėmis“ // http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm; Prisijungimo laikas: 2007-08-29.
24. Direktyvos 95/46/EB 29 str. Darbo grupės 2005 m. rugsėjo 30 d. Nuomonė Nr. 1710/01, WP 112 „Dėl 2004 m. gruodžio 13 d. Tarybos reglamento (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų įgyvendinimo (Nuomonė 2005/3)“// http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm ; Prisijungimo laikas: 2007-08-29.
25. Direktyvos 95/46/EB 29 str. darbo grupės 2007 m. kovo 1 d. Nuomonė Nr. 3/2007, WP 134 „Dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, iš dalies keičiančio diplomatinėms atstovybėms ir konsulinėms įstaigoms skirtas Bendrąsias konsulines instrukcijas dėl vizų atsižvelgiant į biometrinių duomenų įdiegimą, įskaitant nuostatas dėl prašymų išduoti vizą priėmimo ir nagrinėjimo organizavimo (COM (2006) 269 galutinis)“ // http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm ; Prisijungimo laikas: 2007-08-29.
26. 2005 m. rugsėjo 16 d rezoliucija priimta.27-ojoje Tarptautinėje duomenų apsaugos ir privatumo įgaliotinių konferencijoje Montreux "Dėl biometrijos naudojimo pasuose, identifikavimo kortelėse bei kelionės dokumentuose“, // http://www.ada.lt/images/cms/File/rezoliucija_konferencijos_medz.pdf, Prisijungimo laikas: 2007-09-10
27. Europos Parlamento teisėkūros rezoliucija “Dėl Komisijos pasiūlymo dėl Tarybos reglamento dėl ES piliečių pasų apsaugos savybių ir biometrinių duomenų (KOM (2004)0116 – C5-0101/2004 – 2004/0039(CNS))// http://www.europarl.europa.eu/.
28. Enhanced Border Security and Visa Entry Reform Act of 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf Prisijungimo laikas: 2007-11-15.
29. Visa Waiver Program (VWP), US Department of State http://travel.state.gov/visa/temp/without/without_1990.html; Prisijungimo laikas: 2007-10-07.
30. Biometric-Based Technologies, Organisation for Economic Co-operation and Development, Directorate for science, technology and industry, Committee for information, computer and communications, 30-Jun-2004, DSTI/ICCP/REG(2003)2/FINAL, policy http://appli1.oecd.org/olis/2003doc.nsf/43bb6

130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF ; Prisijungimo laikas: 2007-09-10

31. Helllenic Republic Authority for the Protection of Personal Data, Biometric data in International Athens Airport, Decision 52/2003 May 11, 2003. // http://www.dpa.gr/Documents/Eng/Dec%2052%202003%20Biometrics_IAA.doc ; Prisijungimo laikas: 2007-11-27.
32. Directive 95/46/47 article 29 - Data Protection Working Party 2001 December 14 Opinion 10/2001 „On the need for a balanced approach in the fight against terrorism“ // http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf; Prisijungimo laikas: 2007-11-03.
33. Identity Cards Act 2006 (c. 15) // http://www.legislation.gov.uk/acts/acts2006/20060015.htm; Prisijungimo laikas: 2007-11-03.
34. Implementation Plan for the OECD Guidelines for the Security Of Information Systems and Networks: Towards a Culture of Security, Organisation for Economic Co-operation and Development 21-Jan-2003**,** http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/36896c8a5cb63c7ec1256ca6005cf815/$FILE/JT00137968.PDF ; Prisijungimo laikas: 2007-09-10.
35. Inventory of instruments and mechanisms contributing to the implementation and enforcement of the oecd privacy guidelines on global networks, 1999, Paris. // http://www.olis.oecd.org/olis/1998doc.nsf/8d00615172fd2a63c125685d005300b5/23ec07d41a61a5e380256810004dfeab/%24FILE/05E95540.ENG; Prisijungimo laikas: 2007-11-15
36. Ministry of the Interior and Kingdom Relations.Evaluation ReportBiometrics Trial: 2b or not 2b. 2005 // www.minbzk.nl/contents/pages/48403/trailreportbiometrics.doc.pdf ; Prisijungimo laikas: 2007-11-03.
37. Paßgesetz, vom 19. April 1986, BGBl. I S. 537. Aufenhaltstitel, // http://www.aufenthaltstitel.de/passg.html; Prisijungimo laikas: 2007-10-26.

## SPECIALIOJI LITERATŪRA

38. Adler A. Images Can Be Regenerated From Quantized Biometric Match Score Data. 2004 // http://www.sce.carleton.ca/faculty/adler/publications/2004/adler-2004-ccece-quantized-match-score.pdf; Prisijungimo laikas: 2007-10-17.

39. Radvilaitė A. Biometriniai pasai – padidinto saugumo priemonė?, 2006 // http://www.lrytas.lt/?id=11572917321155418560&view=4; Prisijungimo laikas: 2006-11-04.
40. Progress report on the application of the principles of convention 108 to the collection and processing of biometric data. Strasbourg: February 2005 // http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/O-Biometrics(2005)_en.asp; Prisijungimo laikas: 2005-06-14.
41. Albrecht A. Walsh M. Report on legal and privacy issues, BioVision. 2003 // http://www.biteproject.org/documents/biovision-privacy-issues.pdf ; Prisijungimo laikas: 2006-10-11.
42. Analysis and Impact Study on Implementation of Directive 95/46/EC in Member States // ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf; Prisijungimo laikas: 2007-11-27.
43. Bier W. C. Right of Privacy. Fordham Univ Press. 1980. // http://books.google.com/books?id=rofFPZc0nooC&pg=PA196&dq=%22%22; Prisijungimo laikas: 2007-10-17.
44. Bloustein E. Privacy as an Aspect of Human Dignity:: An answer to Dean Prosser.New York: New York University Law review, 1964.
45. Bowyer K. W. Face recognition technology: Security versus privacy. IEEE Technology and Society Magazine. 2003 Nr. 1(23), P. 9 // http://www.cse.nd.edu/Reports/2004/TR-2004-21.pdf; Prisijungimo laikas: 2007-10-23.
46. Mickevičius H. Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą. 2006. // http://www.hrmi.lt/news.php?strid=1999&id=3455 Prisijungimo laikas: 2007-08-29.
47. Cavoukian A. Privacy And Biometrics. Ontario, September 1999 // http://www.pcpd.org.hk/english/infocentre/files/cakoukian-paper.doc
48. Civilka M. Asmens duomenų apsauga tarptautinėje ir EB teisėje// http://www.teisininkas.lt/downloads/ADA_1.12.pdf ; Prisijungimo laikas: 2007-10-14.
49. Clarke R. Privacy Impact Assessments, 2003. // Http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html; Prisijungimo laikas: 2006-10-07.
50. Custers B.H.M. The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Tilburg: Wolf Legal Publishers, 2004.

51. Elgesem D. Privacy, Respect for Persons, and Risk // Philosophical Perspective on Computer Mediated Communication. New York State University of New York Press, 1996. // http://books.google.com/books?id=5IvvWDXBcakC&dq=%22; Prisijungimo laikas; 2007-10-17
52. Biometrics in Europe: Trend Report. European Biometrics Portal, 2006. // http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf; Prisijungimo laikas; 2007-08-29.
53. Introduction of ePassports. National Audit Office, 2007. http://www.nao.org.uk/pn/06-07/0607152.htm; Prisijungimo laikas: 2006-10-11.
54. Gasson M., Meints M. A study on PKI and biometrics, Fidis // Future of identity in the Information Society, 2005.
55. Grijpink J. Privacy law biometrics and privacy: Intro to biometric // Computer Law and Security Report, 17(3), P.154–160, 2001.
56. Gavison R. Privacy and the Limits of the Law // Yale Law Journal., Vol 89, No. 3, 1980.
57. Guerrier C., Cornelie L-A. Les aspects juridiques de la biometrie // http://www.biometrie-online.net/dossiers/generalites/droit/Claudine%20GUERRIER.pdf; 2007-09-23.
58. Hes R., Borking T. Privacy Enhancing Technologies: The Path to Anonymity,.Hague: Registratiiekamer, 1998 // http://66.102.1.104/scholar?q=cache:WEeBHFbtzEMJ:www.cbpweb.nl/documenten/av_11_Privacy-Penhancing_technologies.html; Prisijungimo laikas: 2007-10-17.
59. Hert P. Biometrics: legal issues and implications. Sevilla: 2005 // cybersecurity.jrc.es/docs/LIBE%20**Biometrics**%20March%2005/**Legal**Implications_Paul_de_Hert.pdf; Prisijungimo laikas: 2007-09-11.
60. Hornung G. Biometric Identity Cards: Technical, Legal, and Policy Issues, 2004. //
61. www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/Hornung_Buch_ISSE_2004.pdf Prisijungimo laikas: 2006-10-11.
62. Strategic Action Plan for the National Identity Scheme: Safeguarding your identity. 2006 // http://www.ips.gov.uk/passport/downloads/Strategic_Action_Plan.pdf; Prisijungimo laikas: 2007-11-03.
63. John D. W. Biometrics: Identifying Law &Policy Concerns in Biometrics // http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf; Prisijungimo laikas: 2007-10-05.

64. The Bioprivacy Initiative: A Framework For Evaluating The Privacy Impact Of Biometric Deployment And Technologies. International Biometric Group, 2002. // http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/14-Bio-Privacy.pdf; Prisijungimo laikas: 2007-09-12.
65. The Policy Laundering Project. // http://www.policylaundering.org/keyplayers/ICAO-issues.html, Prisijungimo laikas: 2007-10-05.
66. Sullivan, Clare The United Kingdom Identity Cards Act 2006 – proving Identity?, MqJBL (2006) Vol 3, p. 259-287, http://www.law.mq.edu.au/html/MqJBL/vol3/12Sullivan.pdf
67. Korff D. EC Study on Implementation of Data Protective Directive: Comparative Study of National Laws. Colchester: Human Rights Centre. September, 2002 // http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf; Prisijungimo laikas: 2007-11-14.
68. Rosenzweig P., Kochems A., Schwartz A. Biometric technologies: Security, legal, and policy implications // Legal Memorandum, vol.12, 2004. // http://www.heritage.org/Research/HomelandSecurity/lm12.cfm; Prisijungmo laikas: 2006-09-18.
69. Pankanti S., Prabhakar S., Jain A. K. Biometric recognition: Security and privacy concerns. 2003.
70. Ratha N. K., Connell J. H., Bolle R. M. Enhancing security and privacy in biometrics-based authentication systems, 2001. // http://www.research.ibm.com/journal/sj/403/ratha.html; Prisijungimo laikas: 2007-10-04.
71. Snider M. Repor: Security & Privacy in Large Scale Biometirc System. Brussels: European Biometrics Forum, 2006, http://www.eubiometricsforum.com/dmdocuments2/SecurityPrivacyWorkshopReportvs4DEF.doc; Prisijungimo laikas: 2006-10-11.
72. International Organization for Migration. Biometrics and International Migration.// International Migration Law, No.5, 2005. // www.unitarny.org/mm/File/**Biometrics**.pdf; Prisijungimo laikas: 2006-10-11.
73. Biometrics at the Frontiers: Assessing the Impact on Society. 2005 // ec.europa.eu/justice_home/doc_centre/freetravel/doc/**biometrics**_eur21585_en.pdf; Prisijungimo laikas: 2006-08-27.
74. Miller B. Vital signs of identity.// IEEE Spectrum: Vol. 31, No. 2, 1994.
75. Nanavati S., Thieme M., Nanavati R. Biometrics. Identity Verification in a Networked World. New York: A Wiley Tech Brief Wiley Computer Publishing, 2002.

76. Nissenbaum H., The Meaning of Anonymity in an Information Age. // The Information Society, Nr.15. 1999.
77. Prahbakar S ir kt. Biometric Recognition: Security and Privacy Concerns // http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf; Prisijungimo laikas: 2007-10-27.
78. Rejman-Greene M. Roadmap for Biometrics in Europe to 2010, BioVision, 2003. // http://ftp.cwi.nl/CWIreports/PNA/PNA-E0303.pdf; Prisijungimo laikas: 2007-10-19
79. Shorter Oxford English Dictionary: Sixt Edition . Oxford University Press, 2006.
80. Mitsilegas V. Controlling foreigners, passengers, citizens: surveillance and counter-terrorism, 2005. // http://www.utexas.edu/cola/centers/european_studies/conferences/immigration_policy/papers/noformat/conferences/immigration_policy/PDF/papers/mitsiligas.pdf; Prisijungimo laikas: 2006-10-29.
81. Wayman, J. L., ir kt. Biometric Systems: Technology, Design and Performance Evaluation. London: Springer-Verlag, 2005.
82. Weichert T. Staatliche Identifizierung durch Biometrie // Datenschutz, Vol. 2, 2004.
83. Grossman W. M. Is school fingerprinting out of bounds?, 2003 // http://www.guardian.co.uk/technology/2006/mar/30/schools.guardianweeklytechnologysection; Prisijungimo laikas: 2007-11-07.
84. Woodward J. D. Biometrics: Privacy's foe or privacy's friend? // Proceedings of the IEEE, Nr. 9, 1997. // http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf Prisijungimo laikas: 2007-11-07.

Santrauka

Biometrija ir asmens duomenų apsauga: teisiniai aspektai

Magistro baigiamajame darbe yra nagrinėjama Lietuvoje mažai analizuota asmens duomenų apsaugos taikant biometrines tapatybės nustatymo priemones problematika. Biometrinės technologijos buvo pradėtos ypač plačiai taikyti pirmojo dešimtmečio pradžioje ir iš karto sukėlė intensyvias diskusijas dėl savo santykio su žmogaus teisių apsaugos standartais. Žmogaus fiziniais parametrais paremtos technologijos įgalina mažais kaštais rinkti ir saugoti didelių žmonių grupių asmeninę informaciją.

Biometrijos naudojimo problematika yra labai plati, todėl darbe yra koncentruojamasi į vieną pagrindinį aspektą – biometrijos teisinį reglamentavimą. Darbe atskleidžiama ES ir tarptautiniu taikoma asmens duomenų saugumo samprata, bei jos sąlygojami biometrinių technologijų naudojimo apribojimai. Daug dėmesio yra skiriama biometrinių duomenų rinkimo, saugojimo ir naudojimo sąlygojamų grėsmių analizei. Taip pat išsamiai aptariamos technologinės biometrijos ypatybės bei jų sąlygojami apribojimai. Atsižvelgiant į šias galimybes ir apribojimus yra atliekama išsami tarptautinių susitarimų biometrijos srityje analizė bei išskiriami pagrindiniai biometrijos naudojimo principai. Šiame kontekste yra analizuojama ES pradėtas biometrinių pasų diegimas bei aptariamos dvejų didžiųjų ES valstybių – Vokietijos ir D.Britanijos įgyvendinamos biometrinių duomenų naudojimo politikos.

Darbas sąlygoja keletą pagrindinių išvadų. Pažymėtina, jog biometrijos naudojimas, dėl ypatingo šių duomenų pobūdžio nuo pat technologijos užuomazgų yra susijęs su atitinkamu valstybių dėmesiu bei pastangomis sukurti jį lydinčius principų rinkinius. Antra, technologinių biometrijos naudojimo galimybių analizė rodo, jog ši identifikavimo metodika turi nemaža trūkumų, todėl pati biometrinė metodika negali būti laikoma visiškai patikima, o klaidingo identifikavimo kaštai gali būti ženklūs. Todėl, atsižvelgiant į šias aplinkybes, biometrinių technologijų taikymas yra siejamas su papildomų identifikavimo metodų egzistavimu.

Summary

Biometry and Personal Data Protection: Legal Aspects

This Master thesis is focused on the legal aspects of biometry application and human rights protection, a new topic, still attracting little researchers' attention in Lithuania. Rapid emergence of biometry technologies in the early 2000's in response to the need for effective personal identification measures has raised multiple concerns over their compatibility with human data protection standards. The key issues addressed in this debate are the relation between the use and storage of biometric data with the concepts of privacy, the protection of personal data and security of stored information.

The field of biometry application is very wide, therefore in this paper it is focused primarily on one key issue – the legal regulation of biometrics. Pursuing this topic the international and European concepts of personal data protection are analysed, as well as the limitations, associated with the application of biometric technologies. Significant attention is devoted to the threats posed by the collection, processing and storage of biometric data. Further to that the technological aspects of biometry are also discussed. Basing on these limitations and opportunities a comprehensive analysis of international agreements in the field of biometry is conducted and the key principles, ruling the use of biometry are defined. In this context also the EU policies in the fields of biometric passports are discussed as well as German and British policies.

The paper draws several conclusions. First it is noted that the application of biometry from its very conception is followed by the development of respective international agreements and international efforts to develop corresponding sets of principles. Second, the analysis of biometry application shows that this technology has significant backlogs, therefore it must be used only with parallel modes of identification and must not be considered as reliable *per se*.