



**Darbinis dokumentas dėl biometrinių duomenų**

**Priimta 2003 m. rugpjūčio 1 d.**

Darbo grupė buvo įsteigta vadovaujantis Direktyvos 95/46/EB 29 straipsniu. Tai nepriklausomas ES patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai išdėstyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 97/66/EB 14 straipsnyje.

Sekretoriatą suteikia Europos komisijų direktoratas (Vidaus rinkos funkcionavimas ir poveikis. Koordinavimas. Duomenų apsauga), Vyriausiasis vidaus rinkos direktoratas. B-1049 Brussels – Belgium – Office C100-6/136  
Interneto adresas: <http://www.europa.eu.int/comm/privacy>

## DARBO GRUPĖ ASMENŲ APSAUGAI TVARKANT ASMENS DUOMENIS

Įkurta pagal 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EC<sup>1</sup>, atsižvelgiant į Direktyvos 29 ir 30 straipsnių 1(a) ir 3 paragrafus, atsižvelgiant į jos Procedūros taisykles, ypač į 12 ir 14 straipsnius,

**priėmė šį Darbinį dokumentą:**

### 1. ĮVADAS

Greitas biometrinių technologijų vystymasis ir pastaraisiais metais paplitęs pritaikymas reikalauja atidaus jų nagrinėjimo duomenų apsaugos požiūriu<sup>2</sup>. Platus ir nekontroliuojamas biometrinių duomenų naudojimas kelia susirūpinimą dėl individų pagrindinių teisių ir laisvių apsaugos. Šie duomenys yra ypatingi, kadangi yra susiję su individo elgesio bei psichologinėmis charakteristikomis ir leidžia jį ar ją identifikuoti<sup>3</sup>.

Biometriniai duomenys šiuo metu yra dažnai naudojami automatinio autentifikavimo/verifikavimo bei tapatybės nustatymo procedūrose, ypač kontroliuojant įėjimą į fizines ir virtualias zonas (pvz., priėjimas prie tam tikrų elektroninių sistemų ar paslaugų).

Anksčiau biometriniai duomenys buvo naudojami iš esmės DNR ir pirštų atspaudų testavimui. Pirštų atspaudai daugiausia buvo renkami įstatymų įgyvendinimo tikslais (pvz., baudžiamojo tyrimo tikslais). Jei visuomenė skatins pirštų atspaudų ar kitų biometrinių duomenų bazių plėtrą tolesniam taikymui, trečiosios šalys potencialiai gali imti dažniau tokius duomenis pakartotinai naudoti lyginimo ar tyrimo tikslu be pradinio tokio tikslo nustatymo; šios trečiosios šalys gali būti ir įstatymo įgyvendinimo institucijos.

Ypatingą rūpestį dėl biometrinių duomenų kelia tai, kad vis plačiau naudojant tokius duomenis visuomenė gali nebejausti šių duomenų tvarkymo poveikio kasdieniam gyvenimui. Pavyzdžiui, dėl biometrinių duomenų naudojimo mokyklų bibliotekose, vaikai gali nebekreipti dėmesio į duomenų apsaugai kylančias grėsmes, kurios gali paveikti jų tolesnį gyvenimą.

Šio dokumento tikslas yra prisidėti prie efektyvaus ir vienodo nacionalinių duomenų apsaugos nuostatų, priimtų remiantis Direktyva 95/46/EB, taikymo biometrinėms sistemoms. Šis dokumentas daugiausia dėmesio skirs biometrinių duomenų pritaikymui autentifikavimo ir verifikavimo tikslais. Darbo grupė siekia pateikti Europai bendras gaires, ypač biometrinių sistemų industrijai ir tokių technologijų naudotojams.

<sup>1</sup> Official Journal no. L281, 1995-11-23, p. 31, prieinamas adresu: [http://europa.eu.int/comm/internal\\_market/privacy/law\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law_en.htm)

<sup>2</sup> Nuo 2001 m. rugsėjo 11 d. biometriniai duomenys dažnai vadinami geromis visuomenės saugumo priemonėmis. Europos Sąjungoje vyksta diskusijos dėl biometrinių duomenų įtraukimo į identifikavimo korteles, pasus, kelionės dokumentus ir visas. JAV greitai laiku reikalaus biometrinių identifikatorių iš užsieniečių, šiems atvykstant į šalį arba išvykstant iš jos. ILO Konvencija Nr. 108 buvo pakeista 2003 m., kad jūrininkams taptų privaloma pateikti savo biometrinius duomenis. Taip pat diskusijos vyksta ir kituose tarptautiniuose forumuose, tokiuose kaip G8, OECD ir kt.

<sup>3</sup> Unikalus identifikavimas priklauso nuo skirtingų faktorių, įskaitant duomenų bazės dydį ir naudojamų biometrinių duomenų tipo.

## 2. Biometrinių sistemų apibūdinimas

Biometrinės sistemos yra biometrinių technologijų pritaikymas, kuris leidžia automatiškai nustatyti asmens tapatybę ir/ar autentifikuoti/verifikuoti<sup>4</sup> asmenį. Autentifikavimas/verifikavimas yra dažnai naudojamas įvairiais tikslais visiškai skirtingose srityse ir priklauso plataus spektro subjektų atsakomybei.

Kiekvienas biometrinis duomuo, nepriklausomai autentifikavimo/verifikavimo ar tapatybės nustatymo, daugiau ar mažiau priklauso nuo konkrečių biometrinių duomenų:

- **universalijų:** tokius biometrinius elementus turi visi asmenys<sup>5</sup>;
- **unikalių:** kiekvieno asmens biometrinis elementas yra skirtingas;
- ir **pastovių:** asmens biometrinio elemento savybė išlieka pastovi visą laiką.

Dvi pagrindinės biometrinių technologijų kategorijos skiriamos pagal tai, ar yra naudojami<sup>6</sup> pastovūs, ar kintantys elgesio duomenys.

Pirmiausia yra skiriamos fizinės ir **fiziologiniais požymiais besiremiančios** technologijos, kurios lygina asmens fiziologines charakteristikas ir apima: pirštų atspaudų patikrinimą ir analizę, akies rainelės atpažinimą, tinklainės analizę, veido ir delno kontūro atpažinimą, ausies formos, kūno kvapo, balso atpažinimą, DNR analizę<sup>7</sup> ir prakaito porų analizę, ir pan.

Antra, yra **elgesio ypatybėmis** paremtos technologijos, kurios lygina asmens elgesio ypatybes ir apima ranka rašyto parašo verifikavimą, klaviatūros klavišų spaudimo analizę, eisenos analizę ir pan.

Atsižvelgiant į greitą technikos evoliuciją ir išaugusį rūpestį dėl saugumo, daug biometrinių sistemų dirba jungdamos skirtingus biometrinius vartotojo modalumus su kitomis tapatybės nustatymo ar autentiškumo patvirtinimo technologijomis. Kai kurios sistemos, pavyzdžiui, sujungia veido atpažinimą ir balso registravimą. Autentifikavimui gali būti kartu naudojami trys skirtingi metodai – pirmasis remiasi tuo, ką individas žino (slaptažodis, PIN, t.t.), antrasis – tuo, ką individas turi (žetonas, CAD raktas, kortelė, t.t.) ir trečiasis – tuo, kas individas yra (biometrinis požymis). Pavyzdžiui, kompiuterio pagalba kas nors gali įdėti kortelę, surinkti slaptažodį ir pateikti savo piršto atspaudą.

Biometrinių pavyzdžių, vadinamųjų biometrinių duomenų (piršto atspaudų vaizdo, tinklainės ar rainelės vaizdo, balso įrašo), rinkimas yra atliekamas vadinamoje „registracijos“ fazėje, kiekvienam biometrinių duomenų tipui naudojant konkretų daviklį. Biometrinė sistema iš

<sup>4</sup> Skirtumas tarp autentifikavimo (verifikavimo) ir tapatybės nustatymo yra labai svarbus. Autentifikavimas atsako į klausimą: Ar aš tas, kuriuo bandau prisistatyti? Sistema patvirtina asmens tapatybę, tvarkydama biometrinius duomenis, kurie susiję su asmeniu, kuris klausia ir priima taip/ne sprendimą (1:1 palyginimas). Tapatybės nustatymas atsako į klausimą: Kas aš esu? Sistema atpažįsta klausiantįjį individą, išskirdama jį iš kitų asmenų, kurių biometriniai duomenys taip pat yra saugomi. Šiuo atveju sistema priima vieną iš n sprendimų ir atsako, kad klausiantysis asmuo yra X.

<sup>5</sup> Šiuo atveju ne visi biometriniai elementai yra lygiareikšmiai ir vieno asmens išskyrimo iš kitų asmenų rodikliai yra labai skirtingai, atsižvelgiant į naudojamų biometrinių duomenų tipą. Labiausiai besiskiriantys biometriniai elementai yra DNR, tinklainė ir pirštų atspaudai.

<sup>6</sup> Kai kurios technologijos gali remtis ir fiziologiniais, ir elgesio ypatybėmis.

<sup>7</sup> Nors DNR naudojimas biometriniams tapatybės nustatymui iškelia specifinius klausimus, tokios diskusijos į šį dokumentą neįtrauktos. Galima tik paminėti, kad šiuo metu neatrodo įmanomas DNR, kaip autentifikavimo priemonės, apibūdinimo generavimas realiu laiku.

turimų biometrinių duomenų išskiria konkrečius naudotojo požymius, kad galėtų sukurti biometrinių „modelių“. Modelis yra biometrinio atvaizdo struktūrinis sumažinimas: užfiksuoti individo biometriniai matmenys. Tai yra skaitmeninis modelis, kuris bus saugomas ir kuris pats nėra biometrinis elementas. Be to, atsižvelgiant į naudojamos biometrinės sistemos funkcionavimą<sup>8</sup>, biometriniai duomenys gali būti tvarkomi kaip neapdoroti duomenys (atvaizdas).

Registracijos fazė yra labai svarbi, kadangi tik joje vienu metu kartu yra: neapdoroti duomenys, atrinkimo ir apsaugos algoritmai (kriptografija, maiša ir pan.) bei modeliai. Ryšium su tuo reikia pažymėti, kad jei neapdoroti duomenys atskleidžia informaciją, kuri pagal Direktyvos 95/46/EB 8 straipsnį gali būti vertinama kaip ypatingi duomenys, tai tokių duomenų registracijos procesas turi vykti vadovaujantis šia nuostata (žr. žemiau 3.7 punktą).

Duomenų apsaugos požiūriu taip pat labai svarbus yra vartotojų modelių saugojimo būdo klausimas. Tai priklauso nuo biometrinio prietaiso naudojimo būdo ir pačių modelių dydžio. Modeliai gali būti saugomi:

- a) biometrinio įrenginio atmintyje;
- b) centrinėje duomenų bazėje;
- c) plastikinėse kortelėse, optinėse kortelėse ar mikroprocesorinėse kortelėse. Šis saugojimo metodas leidžia vartotojams nešiotis savo modelius su savimi, kaip tapatybės nustatymo priemonę.

Iš esmės autentifikavimo/verifikavimo tikslais nebūtina saugoti apibūdinančius asmenį duomenis duomenų bazėje; pakanka saugoti asmens duomenis necentralizuotu būdu. O tapatybė gali būti nustatoma tik saugant asmenį apibūdinančius duomenis centralizuotoje duomenų bazėje, kadangi nustatydamas duomenų subjekto tapatybę sistema turi palyginti jo/jos modelį ar neapdorotus duomenis (atvaizdą) su visų asmenų, kurių duomenys jau yra centralizuotai saugomi, modeliais ar neapdorotais duomenimis.

Kitas duomenų apsaugos požiūriu svarbus dalykas yra faktas, kad kai kurios biometrinės sistemos remiasi informacija, kaip antai pirštų atspaudai ar DNR, kuri gali būti renkama be duomenų subjekto žinios, kadangi ji ar jis to nežinodami gali palikti pėdsakus. Pritaikant biometrinių algoritmą pirštų atspaudams, rastiems ant stiklo, kas nors gali nustatyti<sup>9</sup>, ar asmuo yra įtrauktas į biometrinių duomenų bazę, ir jeigu taip, tai toliau lyginant modelius nustatyti, kas jis yra. Tai taikytina ir kitoms biometrinėms sistemoms, pavyzdžiui, kurios analizuoja klaviatūros klavišų spaudimą ar atpažįsta veidą per atstumą, atsižvelgiant į naudojamų technologijų specifinius požymius<sup>10</sup>. Probleminis aspektas yra tas, kad, viena vertus, duomenys gali būti tvarkomi be duomenų subjekto žinios ir kad nepaisant jų dabartinio patikimumo, šios biometrinės technologijos gali būti pilnai panaudotos dėl jų nežymaus įsikišimo. Todėl, atrodo, yra būtina nustatyti joms konkrečias saugumo priemones.

<sup>8</sup> Šis dokumentas daugiausia taikomas modeliais paremtoms biometrinėms sistemoms ir gali būti taikomas neapdorotiems duomenims. Neapdorotų duomenų specifika gali sąlygoti duomenų apsaugos reikalavimų supaprastinimą.

<sup>9</sup> Tačiau tai reiškia bent jau konkrečias priemones, leidžiančias nuo stiklo paviršiaus surinkti pirštų atspaudus nepažeidžiant jų, techninę įrangą pirštų atspaudų duomenų tvarkymui, priėjimą prie konstruktoriaus algoritmo ir/ar pirštų atspaudų duomenų bazės.

<sup>10</sup> Žr. 3 nuorodą dėl Direktyvos 95/46/EB taikymo ir ypač 3.3 nuorodą dėl prievolės informuoti duomenų subjektą.

### 3. DIREKTYVOS 95/46/EB PRINCIPŲ TAIKYMAS

#### 3.1. Direktyvos 95/46/EB taikymas

Direktyvos 95/46/EB 2 a) straipsnis apibrėžia „asmens duomenis“ kaip „bet kurią 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 ir netiesiogiai, ypač pasinaudojus nurodytu asmens identifikavimo kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais“. 26 išvardijimas papildomai paaiškina, kad „norint nustatyti, ar asmens tapatybė gali būti nustatyta, reiktų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti“.

Remiantis šiuo apibrėžimu, tapatybės nustatymo biometrinės priemonės ar jų skaitmeninis perkėlimas į modelį daugeliu atvejų yra asmens duomenys<sup>11</sup>. Taigi atrodo, kad biometriniai duomenys visada gali būti vertinami kaip „informacija, susijusi su fiziniu asmeniu“, nes jie pagal savo pobūdį teikia informaciją apie konkretų asmenį. Biometrinio tapatybės nustatymo kontekste, paprastai asmens tapatybė yra nustatoma, jei tapatybės nustatymui ar autentifikavimui/verifikavimui yra naudojami biometriniai duomenys, bent jau ta prasme, kad duomenų subjektas yra išskiriamas iš visų kitų<sup>12</sup>. Biometrinis asmens tapatybės nustatymas yra toks, kai tapatybės nustatymui ar autentifikavimui/verifikavimui yra naudojami biometriniai duomenys, išskiriantys duomenų subjektą iš visų kitų asmenų.

Pagal Direktyvos 95/46/EB 3 straipsnio 1 paragrafą, duomenų apsaugos principai taikomi automatiniais būdais tvarkant asmens duomenis ištiesai arba dalimis ir neautomatiniais būdais tvarkant asmens duomenis, kai tie duomenys sudaro arba yra skirti sudaryti rinkmenų sistemos dalį. Direktyva netaikoma, kai duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine veikla. Tai tinka ir daugeliui biometrinių duomenų, naudojamų namų ūkyje.

Be šių konkrečių išimčių, biometrinių duomenų tvarkymas laikomas teisėtu, jei visos procedūros, pradedant registracija, yra atliekamos remiantis Direktyvos 95/46/EB nuostatomis.

Šis dokumentas neapima visų klausimų, kurie iškyla biometriniais duomenims taikant Direktyvą 95/46/EB. Yra aptarti tik patys reikšmingiausi ir todėl nėra pilno Direktyvos 95/46/EB taikymo pasekmių vaizdo.

#### 3.2. Tikslų ir proporcingumo principas

Pagal Direktyvos 95/46/EB 6 straipsnį, asmens duomenys turi būti renkami įvardytais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais. Be to, asmens duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti (tikslų principas).

Laikantis šio principo pirmiausia reikia aiškiai išskirti tikslą, kuriuo biometriniai duomenys yra renkami ir tvarkomi. Toliau yra būtinas proporcingumo ir teisėtumo įvertinimas, atsižvelgiant į riziką individų pagrindinių teisių ir laisvių apsaugai ir ypač į tai, ar numatomas

<sup>11</sup> Tais atvejais, kai biometriniai duomenys, pvz., modelis, yra saugomi taip, kad duomenų valdytojas ar bet kuris kitas asmuo negali panaudoti jokių priemonių, kad identifikuotų duomenų subjektą, šie duomenys neturi būti kvalifikuojami, kaip asmens duomenys.

<sup>12</sup> Asmens identifikavimo galimybė priklauso ir nuo kitų duomenų, kurie, kartu ar atskirai, leidžia aptariamą asmenį identifikuoti. „Tiesioginio identifikavimo“ galimybė „vieno ar daugiau jo fizinei tapatybei būdingų veiksnių“ priemonėmis yra aiškiai paminėta Direktyvos 95/46/EB 2a straipsnio asmens duomenų apibrėžime.

tikslas gali būti pasiektas mažiau braunantis į privatumą. Proporcingumo kriterijus visada buvo pagrindinis beveik visuose iki šiol duomenų apsaugos institucijų priimtuose sprendimuose dėl biometrinių duomenų tvarkymo<sup>13</sup>.

Dėl autentifikavimo/verifikavimo Darbo grupė laikosi nuomonės, kad biometrinės sistemos, susijusios su pėdsakų nepaliekančiomis fizinėmis charakteristikomis (pvz., rankos kontūras, bet ne pirštų atspaudai), arba biometrinės sistemos, susijusios su pėdsakus paliekančiomis fizinėmis charakteristikomis, bet išimenančios niekieno kito, o tik aptariamojo individo duomenis (kitai sakant, duomenys nėra išimunami prieigos kontrolės įrenginyje ar centrinėje duomenų bazėje), sukuria mažesnę riziką pagrindinėms asmens teisėms ir laisvėms<sup>14</sup>. Keletas duomenų apsaugos institucijų pritarė šiam požiūriui, pareikšdamos, kad pageidautina, jog biometriniai duomenys nebūtų saugomi duomenų bazėje, o tik išskirtinai vartotojui prieinamame objekte, pavyzdžiui, mikroprocesorinėje kortelėje, mobiliajame telefone, banko kortelėje<sup>15</sup>. Kitaip tariant, autentifikavimui/verifikavimui, kuris gali būti atliekamas be centrinio biometrinių duomenų saugojimo, neturi būti piktnaudžiuojama identifikavimo technologijomis.

Be to, Darbo grupė mano, kad kitokie taikymo būdai (pavyzdžiui, paremti skaitmeniniais pirštų atspaudų modeliais terminale ar centrinėje duomenų bazėje) turi būti atidžiai įvertinti prieš tokių taikymo būdų panaudojimą. Tačiau, jei ši sistema bus įgyvendinama, pvz., sustiprintos apsaugos įrenginiuose<sup>16</sup>, tai gali būti vertinama, kaip riziką sukeliantis duomenų tvarkymas, kaip tai suprantama pagal Direktyvos 95/46/EB 20 straipsnį, ir pagal nacionalinės teisės nuostatas (žr. 3.5 nuorodą) yra reikalinga pateikti duomenų apsaugos institucijoms išankstinei patikrai.

Direktyva 95/46/EB draudžia tolesnį tvarkymą, kuris nėra suderintas su duomenų rinkimo tikslu. Pavyzdžiui, tada, kai biometriniai duomenys yra tvarkomi priėjimo kontrolės tikslais, tokių duomenų naudojimas duomenų subjekto emocinės būklės įvertinimui ar stebėjimui darbo vietoje būtų nesuderinamas su pradiniu rinkimo tikslu. Turi būti imtasi visų priemonių nuo tokio netinkamo panaudojimo<sup>17</sup>. Direktyva 95/46/EB numato išimtį, kai duomenų tvarkymas nesuderintais tikslais nedraudžiamas, bet tam taikomos konkrečios sąlygos.

Yra bendra nuomonė, kad biometrinių duomenų, gautų individams nesąmoningai palikus fizinius pėdsakus (pvz., pirštų atspaudus), pakartotinio panaudojimo netinkamais tikslais rizika sąlygiškai yra nedidelė, jei duomenys nėra saugomi centralizuotose duomenų bazėse, bet lieka su asmeniu ir yra neprieinami trečiajai šaliai. Biometrinių duomenų centralizuotas saugojimas taip pat padidina biometrinių duomenų naudojimo kaip raktų, susiejančio skirtingas duomenų bazes, kurios gali leisti apibūdinti individų įpročius, riziką tiek privačiame, tiek ir viešajame sektoriuje. Tinkamo tikslo klausimas iškelia skirtingų biometrinius duomenis naudojančių sistemų sąveikos problemą. Būtinai sąveikos standartizavimas gali sąlygoti didesnę duomenų bazių sąryšį.

#### Biometrinių duomenų naudojimas kelia papildomą kiekvienos tvarkomų duomenų

<sup>13</sup> Pavyzdžiui Olandijos, Prancūzijos, Vokietijos, Italijos ir Graikijos institucijų sprendimai.

<sup>14</sup> Kai kas gali išskirti centralizuotai tvarkomų biometrinių duomenų atvejį, iš atvejo, kai charakterizuojantys duomenys yra saugomi mobiliame įtaise ir palyginimo procesas vyksta kortelėje, bet ne daviklyje, ar net kai daviklis irgi yra mobilus įtaiso dalis.

<sup>15</sup> Turi būti atsižvelgiama į įrenginius, įdiegtus tam, kad būtų išspręstos problemos, kylančios dėl pamestų, pavogtų ar pažeistų kortelių, ir turi būti siūlomi tokie įrenginiai, kurie nesaugo biometrinių duomenų. Ten, kur įmanoma, duomenys turi būti renkami tiesiogiai iš duomenų subjekto.

<sup>16</sup> Tokia yra dabartinė biometrinių technologijų būklė, kad šiuo metu nėra patikimų, aiškių tapatybės nustatymo sprendimų realiam gyventojų skaičiui ir nepanašu, kad artimiausioje ateityje jų atsiras.

<sup>17</sup> Kaip nurodyta aukščiau, šis tikslas turi būti aiškiai apibrėžtas.

kategorijos proporcingumo klausimą, atsižvelgiant į duomenų tvarkymo tikslą. Biometriniai duomenys gali būti naudojami tik jei jie yra tapatūs, tinkami ir tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti. Tai reikalauja griežto tvarkomų duomenų būtinumo ir proporcingumo įvertinimo<sup>18</sup>. Pavyzdžiui, Prancūzijos CNIL nepritarė pirštų atspaudų naudojimui, kad vaikai galėtų patekti į mokyklos restoraną<sup>19</sup>, bet pritarė rankos kontūro modelio naudojimui minėtu tikslu. Portugalijos duomenų apsaugos institucija neseniai priėmė nepalankų sprendimą dėl biometrinės sistemos (pirštų atspaudų) naudojimo universitete dėl nedėstančių darbuotojų stropumo ir punktualumo kontrolės<sup>20</sup>. Vokietijos duomenų apsaugos institucija priėmė palankų sprendimą dėl biometrinių charakteristikų įdiegimo tapatybės nustatymo dokumentuose, siekiant užkirsti kelią jų padirbinėjimui, numatant, kad palyginimui su savininko pirštų atspaudais reikalingi duomenys bus saugomi kortelės mikroschemoje, o ne duomenų bazėje.

Sunkumų gali iškilti dėl to, kad biometriniai duomenys dažnai apima daugiau informacijos, negu yra būtina tapatybės nustatymui ar autentifikavimui/verifikavimui. Toks būtų originalaus atvaizdo (neapdorotų duomenų) atvejis, kadangi modelis gali ir turi būti techniškai sukonstruotas tokiu būdu, kad neleistų duomenų, kurie nėra būtini, tvarkymo. Nereikalingi duomenys turi būti sunaikinti kuo greičiau<sup>21</sup>. Be to, kai kurie biometriniai duomenys gali atskleisti rasinę kilmę ar sveikatos būklę. (žr. žemiau 3.7 nuorodą).

Pagaliau turi būti paminėta, kad biometrinių sistemų naudojimas gali būti organizuojamas tokiu būdu, kad jos *inter alia* būtų pripažįstamos privatumą skatinančiomis technologijomis, kadangi jos gali sumažinti kitų asmens duomenų, kaip antai vardas, adresas, gyvenamoji vieta ir pan., tvarkymą.

### 3.3. Sąžiningas rinkimas ir duomenų subjekto informavimas

Biometrinių duomenų tvarkymas ir ypač jų rinkimas turi būti sąžiningas<sup>22</sup>. Valdytojas turi informuoti duomenų subjektą pagal Direktyvos 95/46/EB 10 ir 11 straipsnius<sup>23</sup>. Konkrečiai tai apimtų tikslų rinkmenos valdytojo (kuris dažnai bus asmuo, valdantis biometrinę sistemą ar taikantis biometrines technologijas) tapatybės ir tikslo apibūdinimą.

Turi būti vengiama sistemų, kurios renka biometrinius duomenis be duomenų subjektų žinios. Šiuo požiūriu kai kurios biometrinės sistemos, pvz., nuotolinio veido atpažinimo, pirštų atspaudų rinkimo, balso įrašymo, kelia didesnę pavojų.

<sup>18</sup> Tam tikrais atvejais turi būti galimas anonimiškumas ar pseudonimų naudojimas. Turi būti atsižvelgiama į įrenginius, įdiegtus tam, kad išspręstų problemas, kylančias dėl pamestų, pavogtų ar pažeistų kortelių, ir turi būti siūlomi tokie įrenginiai, kurie nesaugo biometrinių duomenų. Ten, kur įmanoma, duomenys turi būti renkami tiesiogiai iš duomenų subjekto.

<sup>19</sup> Atrodo, kad JK duomenų apsaugos institucija pritarė pirštų atspaudų naudojimui panašiomis aplinkybėmis, įgyvendinus tinkamas saugumo priemones.

<sup>20</sup> Portugalijos duomenų apsaugos institucija laikosi nuomonės, kad tokių sistemų taikymas, atsižvelgiant į duomenų tvarkymo tikslą, buvo neproporcingas ir perteklinis. Sistema būtų saugojusi šiuos duomenis biometriniame įrenginyje ir kontroliuojamų asmenų skaičius būtų maždaug 140.

<sup>21</sup> Svarbus ištrynimo pagrindas yra Direktyvos 95/46/EB 6, 1, e) straipsnis, kuris reikalauja saugoti asmens duomenis *ne ilgiau* nei yra reikalinga duomenų tvarkymo tikslais.

<sup>22</sup> Direktyvos 95/46/EB 6 (a) straipsnis.

<sup>23</sup> Pareigos informuoti duomenų subjektą išimties, numatytos Direktyvos 95/46/EB 10 ir 11 straipsniuose, turi būti paremtos teisinėmis priemonėmis ir leisti būtina pareigos informuoti apimtį apribojimą, tam kad būtų garantuoti interesai, išvardyti Direktyvos 95/46/EB 13 straipsnyje (visuomenės saugumas, kriminalinių nusikaltimų prevencija, tyrimas, išaiškinimas ir persekiojimas, ir pan.).

### 3.4. Duomenų tvarkymo teisėtumo kriterijai

Biometrinių duomenų tvarkymas turi būti grindžiamas vienu iš Direktyvos 95/46/EB 7 straipsnyje numatytų teisėtumo principų. Jei rinkmenos valdytojas teisėtumo pagrindu laiko sutikimą, tai Darbo grupė pažymi, kad turi būti laikomasi sąlygų, nustatytų Direktyvos 95/46/EB 2 straipsnyje (bet kuris savanoriškai ir žinomai duotas konkretus duomenų subjekto pareiškimas, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys).

### 3.5. Išankstinė patikra – pranešimas

Kaip jau minėta anksčiau, Darbo grupė remia biometrinių sistemų, kurios neįsidėmi biometrinių pėdsakų terminalinėje prieigos įrangoje ar nesaugo jų centrinėje duomenų bazėje (žr. 3.2 nuorodą), naudojimą. Bet jei yra planuojama naudoti tokias sistemas, Darbo grupė, atsižvelgdama į pakartotinio panaudojimo skirtingais tikslais riziką ir į konkrečias grėsmes prieigos be įgaliojimo atveju, rekomenduoja valstybėms narėms apsvaistyti klausimą dėl jų išankstinės patikros, kurią atliktų duomenų apsaugos institucijos, pagal Direktyvos 95/46/EB 20 straipsnį, kadangi ši tvarkymo rūšis greičiausiai kels konkretų pavojų duomenų subjektų teisėms ir laisvėms. Jei valstybės narės numato įvesti išankstinę patikrą biometrinių duomenų tvarkymui, tai prieš įvedant tokias priemones turi būti tinkamai pasitarta su nacionalinėmis duomenų apsaugos institucijomis.

### 3.6. Saugumo priemonės

Valdytojas, pagal Direktyvos 95/46/EB 17 straipsnį, privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti asmens duomenis nuo netyčinio arba neteisėto sunaikinimo ar praradimo, pakeitimo, neleistino atskleidimo ar prieigos prie jų, ypač kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų. Saugumo priemonės turi būti įgyvendinamos, kai yra tvarkomi (saugomi, perduodami, išrenkamos, palyginamos charakteristikos ir pan.) biometriniai duomenys ir ypač jei valdytojas perduoda tokius duomenis internetu. Saugumo priemonės gali būti sudarytos iš, pavyzdžiui, modelių šifravimo ir šifravimo raktų apsaugos, papildant prieigos kontrolę ir apsaugą, kad virtualiai būtų neįmanoma iš modelių atkurti pradinius duomenis.

Šiuo požiūriu turi būti atsižvelgiama į kai kurias naujas technologijas. Įdomus patobulinimas yra galimybė naudoti biometrinius duomenis kaip šifravimo raktus. Tai iš anksto sukuria 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.

Būtinoms saugumo priemonėms 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. Pavyzdžiui, jei įgaliojoto individo pirštų atspaudai būtų susieti su neįgalio individo tapatybe, pastarasis gali naudotis paslaugomis, prieinamomis pirštų atspaudų savininkui, neturėdamas tam teisės. Tai galėtų būti traktuojama kaip tapatybės vagystė ir, nepriklausomai nuo jos išaiškinimo, individų pirštų atspaudai taptų nepatikimais būsimiems taikymams, tokiu būdu būtų ribojama jo/jos laisvė.

Biometrinėse sistemose pasitaikančios klaidos individui gali turėti kelias pasekmes: klaidingas įgalioto asmens atmetimas ir klaidingas neįgalioto asmens priėmimas gali sukurti rimtų, įvairaus lygio problemų. Vis tik biometrinių duomenų naudojimas turi sumažinti tokių klaidų galimybę. Tačiau taip pat gali būti sukurta iliuzija, kad duomenų subjekto tapatybės nustatymas ar autentifikavimas/verifikavimas visada yra tikslus. Duomenų subjektui gali būti sunku ar net neįmanoma įrodyti, kad yra priešingai. Pavyzdžiui, sistema gali klaidingai identifikuoti duomenų subjektą kaip asmenį, kuriam neturi būti leista skristi ar kuriam neturi būti leista atvykti į šalį ir jis turės labai mažai priemonių išspręsti problemą, kai jam bus pateikti tokie „neginčijami“ prieš jį nukreipti įrodymai. Tokiais atvejais, tai ir vėl turi būti pažymėta, bet koks sprendimas, kuris teisiškai paveikia individą, turi būti priimamas tik po pakartotinio automatinio tvarkymo rezultato patvirtinimo pagal Direktyvos 95/46/EB 15 straipsnį.

Pagaliau, reikia paminėti, kad biometrinių duomenų naudojimas gali pagerinti procedūrų kontrolę, pavyzdžiui, prieigos prie asmens duomenų, susijusių su trečiaisiais asmenimis, atveju, pavyzdžiui, vagystės ir klaidingo panaudojimo (patvirtinimo procedūros).

### 3.7. Ypatingi duomenys

Kai kurie biometriniai duomenys gali būti laikomi ypatingais pagal Direktyvos 95/46/EB 8 straipsnį, ypač duomenys, atskleidžiantys rasinę ar etninę kilmę, arba duomenys apie sveikatą. Pavyzdžiui, veido atpažinimo biometrinėse sistemose gali būti tvarkomi duomenys, atskleidžiantys rasinę ar etninę kilmę. Tokiais atvejais, be bendrų direktyvos apsaugos principų, papildomai bus taikomos specialios apsaugos priemonės, numatytos 8 straipsnyje.

Tai nereiškia, kad bet koks biometrinių duomenų tvarkymas būtinai apims ypatingus duomenis. Klausimas, ar tvarkymas apima ypatingus duomenis, yra fakto klausimas, susijęs su naudojamomis specifinėmis biometrinėmis charakteristikomis ir biometrinių duomenų taikymu. Panašu, kad tai būtų atvejis, kai biometriniai duomenys yra tvarkomi vaizdų forma, kadangi iš esmės, neapdoroti duomenys negali būti atkurti iš modelio.

### 3.8. Unikalus identifikatorius

Biometriniai duomenys yra unikalūs ir dauguma jų sudaro unikalius modelius (ar atvaizdus). Plačiai naudojami, ypač didelei gyventojų daliai, biometriniai duomenys gali būti laikomi bendruoju identifikatoriumi pagal Direktyvą 95/46/EB. Tokiu atveju bus taikoma Direktyvos 95/46/EB 8 straipsnio 7 dalis ir valstybės narės turės nustatyti tokių duomenų tvarkymo sąlygas.

Ten, kur biometrinius duomenis numatyta naudoti kaip raktą asmens duomenis<sup>24</sup> apimančių duomenų bazių susiejimui, gali susidaryti ypač sudėtingos situacijos, kai duomenų subjektas neturės galimybės prieštarauti dėl biometrinių duomenų tvarkymą. Tai dažniausiai gali nutikti santykiuose tarp piliečių ir valstybės institucijų.

Todėl būtų gerai, kad siekiant išvengti asmens duomenų jungimo su kelių duomenų bazių duomenimis per modelių ar skaitmeninių vaizdų palyginimą, modeliai ir jų skaitmeninis vaizdas būtų tvarkomi matematiškai (šifravimas, algoritmai ar tyliosios funkcijos), naudojant skirtingus parametrus kiekvienam biometriniam produktui.

<sup>24</sup> Žr. taip pat ankstesnę 3.2 nuorodą dėl suderinamo pakartotinio panaudojimo.

### 3.9. Elgesio kodeksai ir privatumą skatinančių technologijų (PET) naudojimas

Darbo grupė skatina pramonę gaminti biometrines sistemas, kurios palengvintų rekomendacijų, esančių šiame darbo dokumente, įgyvendinimą ir jei šiai sričiai bus sukurti Europos ar tarptautiniai standartai, jie turi būti suderinti su duomenų apsaugos institucijomis, siekiant skatinti biometrinių sistemų kūrimą, paisant duomenų apsaugos principų, mažinti socialines grėsmes ir neleisti netinkamo biometrinių duomenų naudojimo. Šiame kontekste Darbo grupė pabrėžia privatumą skatinančių technologijų (PET) svarbą, siekiant sumažinti duomenų rinkimą ir neleisti neteisėto tvarkymo.

Be to, Darbo grupė pabrėžia elgesio kodeksų, kurie prisidėtų prie tinkamo duomenų apsaugos principų įgyvendinimo, svarbą, atsižvelgiant į skirtingų sektorių specifines ypatybes, pagal Direktyvos 95/46/EB 27 straipsnį. Bendrijos kodeksai gali būti pateikiami Darbo grupei, kuri, šalia kitų klausimų, nuspręs, ar pateikti projektai yra suderinti su nacionalinėmis duomenų apsaugos nuostatomis, priimtomis vadovaujantis Direktyva 95/46/EB.

### IŠVADOS

Darbo grupė mano, kad dauguma biometrinių duomenų sąlygoja asmens duomenų tvarkymą. Todėl, plėtojant biometrines sistemas, yra būtina atsižvelgti į duomenų apsaugos principus, numatytus Direktyvoje 95/46/EB, atsižvelgiant į ypatingą biometrinių duomenų prigimtį, *inter alia* galimybę rinkti biometrinius duomenis be duomenų subjekto žinios ir neva neabejotiną ryšį su individu.

Proporcingumo principo laikymasis, kuris yra Direktyvoje 95/46/EB užtikrintos apsaugos šerdis, ypač autentifikavimo/verifikavimo kontekste, aiškiai pirmenybę teikia biometrinių duomenų taikymui, kai netvarkomi duomenys, gauti iš individams nežinant paliktų fizinių pėdsakų, ar kai duomenys nesaugomi centralizuotoje sistemoje. Tai leidžia duomenų subjektui geriau kontroliuoti savo asmens duomenų tvarkymą.

Darbo grupė planuoja peržiūrėti šį darbinį dokumentą, atsižvelgiant į duomenų apsaugos institucijų patirtį ir technologijų plėtrą, susijusią su biometrinių duomenų taikymu. Kadangi biometriniai duomenys net ir šiuo metu yra įvairiomis formomis naudojami įvairiose sferose, bus būtina toliau dirbti be atidėliojimų, ypač įdarbinimo, vizų ir imigracijos bei kelionių saugumo kontekste.

Nors už biometrinių sistemų, kurios yra suderintos su duomenų apsauga, plėtojimą lieka atsakinga pramonė, darbinis dialogas tarp visų suinteresuotų šalių, įskaitant duomenų apsaugos institucijas, ypač dėl elgesio kodeksų rengimo, visais atžvilgiais būtų labai naudingas.

Sudarytas Briuselyje, 2003 m. rugpjūčio 1 d.  
Darbo grupei  
*Pirmininkaujantis*  
Stefano RODOTA

Išvertė

B.Jurgelvičienė  
2003-10-