MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO SAUGUMO FAKULTETAS

VALSTYBĖS SIENOS APSAUGOS KATEDRA

OLGA TRUKŠINA

BIOMETRINIŲ ASMENS TAPATYBĖS NUSTATYMO SISTEMŲ PANAUDOJIMO GALIMYBĖS UŽTIKRINANT VISUOMENĖS SAUGUMĄ IR VIEŠĄJĄ TVARKĄ LIETUVOS RESPUBLIKOJE

Magistro baigiamasis darbas

Vadovas

doc. dr. R. Vasiliauskas

KAUNAS, 2013

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO SAUGUMO FAKULTETAS

VALSTYBĖS SIENOS APSAUGOS KATEDRA

BIOMETRINIŲ ASMENS TAPATYBĖS NUSTATYMO SISTEMŲ PANAUDOJIMO GALIMYBĖS UŽTIKRINANT VISUOMENĖS SAUGUMĄ IR VIEŠĄJĄ TVARKĄ LIETUVOS RESPUBLIKOJE

Teisės ir policijos veiklos magistro baigiamasis darbas

Studijų programa 621M90013

Vadovas

_____doc. dr. R. Vasiliauskas

2013 05

Recenzentas

_____

2013 05

Atliko

PVmis1-01 gr. stud.

_____O. Trukšina

2013 04 24

KAUNAS, 2013

TURINYS

ĮVADAS

Prasidėjus XXI amžiui greitas biometrinių technologijų vystymasis ir pastaraisiais metais paplitęs biometrinių asmens tapatybės nustatymo sistemų panaudojimas įvairiose visuomenės veiklos srityse reikalauja atidaus šių sistemų naudojimo probleminių aspektų nagrinėjimo. Sparčiai besivystantis pažangioms technologijoms, taip pat svarbu garantuoti tokios teisinės aplinkos sukūrimą, kurioje būtų ginamos žmogaus teisės ir laisvės.

Po teroro akto, įvykdyto 2001 m. rugsėjo 11 d. Jungtinėse Amerikos Valstijose, visuomenės saugumas, kaip socialinė problema, įgijo naujos svarbos, o šalyse, kur terorizmo grėsmė yra itin didelė, biometrinių asmens tapatybės nustatymo sistemų panaudojimas tapo ypač aktualus. Europos Sąjungos valstybėse bendras požiūris į tarpvalstybines problemas: terorizmą, neteisėtą migraciją, prekybą žmonėmis, organizuotą nusikalstamumą, nusikalstamų veikų prevenciją – paskatino biometrinių asmens tapatybės nustatymo sistemų aktyvesnį naudojimą viešajame, o vėliau ir privačiame sektoriuje.

XX amžiaus pabaigoje-XXI amžiaus pradžioje biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių problemas savo moksliniuose darbuose, monografijose, moksliniuose straipsniuose nagrinėjo tyrėjai: Delac K., Grgic M., Govindaraju V., Grimaldi M., Jain A. K., Zhao W., Barkovskaja J., Bajev O., Belkin R., Vinbegr A., Koldin V., Jonaitis A., Vasiliauskas R., Stupak V., Ivanovas E. ir daugelis kt. Šių ir kitų autorių moksliniais straipsniais ir išaiškinimais remiamasi šiame magistro baigiamajame darbe. Taip pat analizuojami Europos Sąjungos ir nacionaliniai teisės aktai reglamentuojantys tiriamą sritį.

Pažymėtina, kad mokslinės-metodinės literatūros, nagrinėjančios biometrinių asmens tapatybės nustatymo sistemų panaudojimo klausimus ir problemas užtikrinant nacionalinį saugumą, gynybą, visuomenės saugumą, nusikalstamų veikų prevenciją, tyrimą, baudžiamąjį persekiojimą, Lietuvoje praktiškai nėra. Lietuvoje nėra sukurtos vieningos išplėtotos teisinės norminės bazės, reglamentuojančios biometrinių asmens tapatybės nustatymo sistemų naudojimą, menkas visuomenės suvokimas apie biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes.

Temos aktualumą ir pasirinkimą lėmė asmens identifikacijos reikšmingumo augimas visame pasaulyje, o biometrinių asmens tapatybės nustatymo sistemų panaudojimas yra viena iš priemonių, leidžiančių greitai, tiksliai ir efektyviai nustatyti asmens tapatybę.

Šiame magistro baigiamajame darbe nagrinėsime biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių problemas Lietuvoje užtikrinant visuomenės saugumą ir viešąją tvarką.

Tyrimo hipotezė:

Biometrinių asmens tapatybės nustatymo sistemų panaudojimas gali efektyviai padidinti visuomenės saugumo ir viešosios tvarkos užtikrinimo galimybes, tačiau jų praktinis įgyvendinimas Lietuvos Respublikoje nėra plačiai paplitęs.

Tyrimo objektas:

Įvairių šalių mokslinių, teisinių ir praktinių pasiekimų tendencijos biometrinių asmens tapatybės nustatymo sistemų panaudojimo srityje užtikrinant visuomenės saugumą ir viešąją tvarką, šių tendencijų praktinio įgyvendinimo aspektai Lietuvos Respublikoje.

Tyrimo tikslas:

Kompleksiškai išnagrinėti biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių aspektus užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje.

Tyrimo uždaviniai:

1. Išnagrinėti biometrinių asmens tapatybės nustatymo sistemų veikimo principus, šių sistemų panaudojimo aspektus įvairiose pasaulio šalyse užtikrinant visuomenės saugumą ir viešąją tvarką;
2. Nustatyti biometrinių asmens tapatybės nustatymo sistemų praktinio realizavimo galimybes ir pagrindinius biometrinių asmens duomenų tvarkymo teisinio reguliavimo aspektus Europos Sąjungoje ir Lietuvos Respublikoje;
3. Atskleisti visuomenės požiūrį į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje;
4. Pateikti tyrimo išvadas ir pasiūlymus dėl biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje.

Tyrimo metodai:

Tiriant biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių, užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje, probleminius aspektus bei perspektyvas, taikomi šie tyrimo metodai: 1) dokumentų analizės metodas naudojamas analizuojant įvairių pasaulio šalių autorių ir Lietuvos tyrėjų mokslinę literatūrą tiriama tema ir teisės aktus, reglamentuojančius biometrinių asmens duomenų tvarkymą; 2) naudojant lyginamąjį istorinį metodą

siekiama atskleisti biometrinių asmens tapatybės nustatymo sistemų atsiradimą nulėmusias priežastis, šių sistemų panaudojimo poreikio kitimą.; 3) lyginamasis metodas darbe naudojamas lyginant įvairių šalių tyrėjų nuomones, pasaulio šalių patirtį nagrinėjama tema, o teisės aktų lygmeniu - analizuojant Europos Sąjungos ir Lietuvos teisinio reguliavimo problemas tiriamo objekto kontekste; 4) loginis-analitinis metodas naudojamas išsakomiems argumentams susieti ir apibendrinti, metodas taikomas siekiant sukonkretinti, suprasti abstraktų teisės aktuose įtvirtintų nuostatų arba nebaigtų įvardyti aplinkybių, susijusių su biometrinių asmens duomenų tvarkymu, o taip pat pateikiant išvadas ir pasiūlymus; 5) taikant anketinį metodą siekiama atskleisti visuomenės požiūrį ir nuomonę apie biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje; 6) matematinis statistinis metodas darbe taikomas skaičiavimams atlikti, duomenims analizuoti, anketinio tyrimo apklausos rezultatams apibendrinti.

Pagrindinės sąvokos naudojamos darbe: biometrija, biometrinės sistemos, biometriniai skaitytuvai, biometrinis požymis, biometrinis šablonas (modelis), asmens duomenys, asmens biometriniai duomenys.

Darbo struktūra:

Darbą sudaro įvadas, trys skyriai, kurie skirstomi į atskirus poskyrius, išvados ir pasiūlymai. Pirmasis darbo skyrius skirtas atskleisti biometrijos ir biometrinių asmens tapatybės nustatymo sistemų sampratą, šių sistemų atsiradimo istorinę raidą. Nagrinėjami biometrinių asmens tapatybės nustatymo sistemų veikimo principai, šių sistemų panaudojimo pagrindai pasaulio šalyse užtikrinant visuomenės saugumą ir viešąją tvarką. Nagrinėjama biometrinių asmens tapatybės nustatymo sistemų panaudojimo poreikio tema Lietuvoje. Antrajame darbo skyriuje atskleidžiami tiriamos srities teisinio reglamentavimo Europos Sąjungoje ir Lietuvoje pagrindiniai aspektai, analizuojamos pagrindinės asmens duomenų tvarkymo, naudojant biometrines asmens tapatybės nustatymo sistemas, teisinio reguliavimo problemos. Trečiasis darbo skyrius skirtas atskleisti visuomenės požiūrį į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje, apibendrinami 2012-2013m. savarankiškai atlikto anketinio tyrimo gauti rezultatai. Darbo pabaigoje pateikiamos išvados ir pasiūlymai.

1. BIOMETRINĖS ASMENS TAPATYBĖS NUSTATYMO SISTEMOS

1.1. **Biometrinių asmens tapatybės nustatymo sistemų sąvoka**

Biometrija – tai yra mokslo ir technikos sritis, užsiimanti biologinių požymių (fizinių, fiziologinių) matavimu[1]. Biometrijos mokslą išvystė ir biometrijos sąvoką įvedė britų mokslininkai – antropologas, pirštų atspaudų klasifikavimo sistemos kūrėjas Francisas Galtonas (*Francis Galton, 1822–1911*) ir biofizikos pradininkas Karlas Pirsonas (*Carl Pearson, 1857–1936*)[2].

XVII amžiaus viduryje, sparčiai augant miestams, industrinės revoliucijos metu padidėjo ir nusikalstamumas, todėl buvo formaliai pripažinta asmens tapatybės nustatymo problema. Tų laikų teismai, vykdydami teisingumą, jau siekė diferencijuoti bausmės dydį už nusikaltimus padarytus pirmą kartą ir pakartotines nusikalstamas veikas. Tai sąlygojo būtinybę sukurti sistemas, kuriose būtų saugoma informacija apie padarytas nusikalstamas veikas ir nusikaltėlių išorės požymius[3].

Vienas iš pirmųjų tokios sistemos kūrėjų buvo Paryžiaus policijos prefektūros Pirmojo biuro raštininkas Alfonsas Bertiljonas (*Alphonse Bertillon, 1853 – 1914*). Jis 1879 m. pateikė policijos prefektūrai raportą, kuriame išdėstė, kaip neklystamai nustatyti nusikaltėlio tapatybę. A. Bertiljonas, remdamasis belgų mokslininko, vieno iš statistikos mokslo įkūrėjų ir pradininko, Adolfo Ketle (*Adolphe Quetelet, 1796-1874*) moksliškai pagrįstais teiginiais[4], sukūrė išsamią žmogaus išorės požymių klasifikacijos ir jų matavimo sistemą, skirtą nusikaltėliams ieškoti ir atpažinti[5].

XIX amžiuje žmogaus biometrinių požymių matavimai (asmens galvos ir kūno parametrų, randų, apgamų ir kt.) jau buvo taikomi nusikaltėliams nustatyti. 1880 m. Henris Foldsas (*Henry Faulds, 1843–1930*), mokslininkas iš Škotijos, gyvenantis ir dirbantis Japonijoje, tyrė žmogaus pirštų atspaudų įvairumą bei unikalumą ir pasiūlė naudoti šias savybes asmeniui nustatyti. 1901 m. garsiajam Skotland Jarde (angl. *Scotland Yard*) įsikūrė pirmasis „Pirštų atspaudų biuras" (angl. *Fingerprint Bureau*)[6].

---

[1] *Bio* – sudurtinio žodžio pirmoji dalis, reikšmė atitinka žodį „biologinis"; *metrija* – antroji sudurtinio žodžio dalis, rodanti sąsają su matavimu. (Kvietkauskas V. ir kt. Tarptautinių žodžių žodynas. – Vilnius: K. Poželos spaustuvė, 1985. P. 527).

[2] Леонов В. История биометрики и ее применения // Международный журнал медицинской практики, 1999. В.4. Ст. 8.

[3] Torvaldas J. Kriminalistikos keliai ir klystkeliai. – Vilnius: Mintis, 1981. P. 383.

[4] Atskirų žmogaus kūno dalių dydis keičiasi pagal tam tikrus dėsningumus; kiekvieno žmogaus kūno dalių dydžiai yra griežtai individualūs ir nuo tam tikro amžiaus lieka nepakitę; neegzistuoja du žmonės turintys tokius pačius kūno išmatavimus (Torvaldas J. Kriminalistikos keliai ir klystkeliai. – Vilnius: Mintis, 1981. P. 383.).

[5] Ten pat.

[6] Леонов В. История биометрики и ее применения // там же, Ст. 9.

Pirmosios *automatinės sistemos*, galinčios atpažinti asmenį pagal jo vieną ar kitą kūno unikalų požymį, atsirado XIX amžiaus pabaigoje ir buvo pavadintos *biometrinėmis*[7]. Šios sistemos praktiškai nesivystė iki 1960 m., o kai amerikiečiai pasiūlė naudoti sistemą, leidžiančią automatiškai matuoti žmogaus rankos pirštų ilgį – pradėjo vystytis sparčiau.

1963 m. Jungtinių Amerikos Valstijų (toliau JAV) Hughes mokslinių tyrimų institutas (Malibu, Kalifornija) publikuoja straipsnį apie piršto atspaudų automatinį sulyginimą[8].

Dar vėliau, 1960-1970 m., buvo sukurtos biometrinės sistemos, leidžiančios atpažinti žmogų pagal balsą ir parašą[9]. Taigi, *biometrinės sistemos* tai *„prietaisai, kuriuose naudojamos biometrinės technologijos, leidžiančios automatiškai atpažinti asmenį ir (arba) nustatyti jo tapatumą ir (arba) jį patikrinti"* [10].

Tipiška biometrinė sistema yra sudaryta iš integruotų sudedamųjų dalių: `

1. Jutiklio (skaitytuvo), kuris fiksuoja unikalius asmens fizinius ar fiziologinius požymius ir konvertuoja juos į duomenis, kurie gali būti saugomi elektroniniu būdu;
2. Užfiksuoto unikalaus fizinio ar fiziologinio požymio atvaizdo išskyrimo modulio (jutiklio užfiksuotas pirštų atspaudų vaizdas);
3. Užfiksuoto atvaizdo unikalių požymių išskyrimo modulio (signalų apdorojimo algoritmai), kuriame gauti biometriniai duomenys apdorojami siekiant išgauti svarbiausias ir esmines požymio savybes (pvz., papiliarinio rašto padėtis ir orientavimas, papiliarinio rašto individualios detalės, ypatingi požymio taškai);
4. Unikalių požymių apdorojimo algoritmų, kurie atlieka kokybės kontrolės funkciją ir iš surinktų duomenų sudaro biometrinių duomenų šabloną dvejetainio skaitmeninio kodo pavidalu;
5. Biometrinių sistemų duomenų šablonų saugojimo bazės, kurioje saugomi visi surinkti duomenys;
6. Sulyginimo ir sprendimo priėmimo modulio (atitikimo algoritmo), kuriame naujas sudarytas biometrinis šablonas lyginamas su esamais duomenų bazėje šablonais ir pateikiamas atitikimo rezultatas. Sprendimų priėmimo procesas paprastai atliekamas automatiniu būdu (žr. 1 pav.).

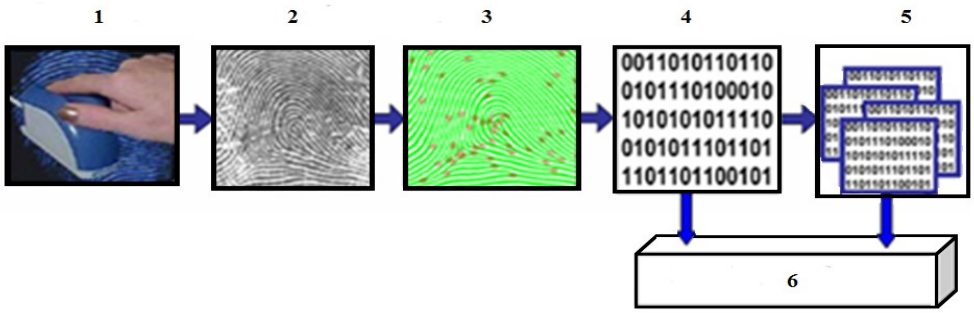
---

[7] Краткая история биометрии // http://www.tadviser.ru/index.php; prisijungimo laikas: 2012-10-01.

[8] Trauring M. Automatic comparison of finger ridge patterns // Hughes Research Laboratories, Report Nr.190. Rev. April, 1963.

[9] Privacy and Data Security Targets of Mytec's Commercialization Strategy // PR Newswire, 1997. P. 24.

[10] Darbinis dokumentas dėl biometrinių duomenų 12168/02/EN WP 80. 29 straipsnio – duomenų apsaugos darbo grupė. 2003 m. rugpjūčio 1d. // http://www.ada.lt/images/cms/File/WP80.pdf; prisijungimo laikas: 2011-11-20.



Šaltinis: http://www.biolink.ru/technology/biometric.phpq1

1 pav. Apibendrinta biometrinės sistemos struktūrinė schema (biometrinis požymis - pirštо atspaudas)

Šiuolaikinės biometrinės sistemos leidžia išskirti ir atpažinti asmenį iš kitų pagal tam tikrus jo fizinius, fiziologinius požymius arba elgesio savybes.

Biometriniu asmens požymiu vadinama unikali jo fizinė, fiziologinė (tarkim, akies rainelės raštas, pirštо pagalvėlės papiliarinis raštas, delno venų išsidėstymas) arba elgsenos (tarkim, kompiuterio klaviatūra renkamo teksto dinamika, balso parametrai, eisenos ypatumai) charakteristika, kurią užfiksuojant yra gaunamas biometrinis požymio pavyzdys[11]. Asmeniui atpažinti tinkami bet kurie išskirtiniai žmogaus biometriniai požymiai.

Po 2001 m. rugsėjo 11 d. teroro išpuolio JAV ir sekančių teroristinių atakų bei išpuolių 2002 m. Maskvoje, 2003 m. Bogotoje, 2004 m. Madride ir Beslane, 2005 m. Londone, pasaulio valstybės pradėjo ieškoti veiksmingų priemonių prieš terorizmo plitimą. Viena iš tokių priemonių tapo biometrinių asmens tapatybės nustatymo sistemų (toliau biometrinės sistemos) panaudojimas.

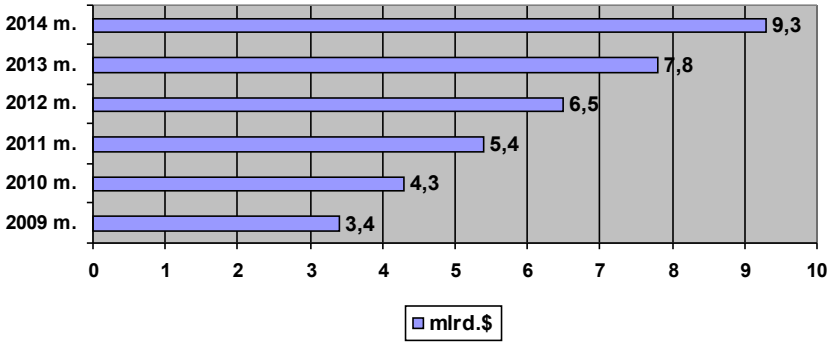
Per pastaruosius 12 metų biometrinių sistemų aktyvus diegimas ir panaudojimas teisėsaugos ir kitose visuomenės veiklos srityse smarkiai užaugo. Literatūros analizė parodė, kad asmens tapatybės nustatymas pagal išorės požymius yra vienas iš svarbiausių faktorių:

- policijos veikloje ir ypatingai kriminalistikoje (pvz., ieškant ir sulaikant besislapstančius nusikaltėlius ir teroristus, atliekant dingusių be žinios asmenų paiešką, tikrinant asmens dokumentus ir pan.);
- užtikrinant kompiuterinės informacijos apsaugą;
- užtikrinant valstybės garantuojamas teises piliečiams ir atvykstantiems į šalį užsieniečiams (atliekant asmens identifikaciją, kai išduodami asmens tapatybę patvirtinantys dokumentai, kertant valstybines sienas, skirstant įvairias socialines išmokas, ir t.t.);
- atsiskaitant už prekes ar paslaugas prekybos įstaigose, naudojantis bankomatų ir prekybos automatų paslaugomis;

[11] Ivanovas E. Biometriniai požymiai asmens atpažinimo sistemose // Mokslas Lietuvos ateitis, 2010. T. 2. Nr. 1. P. 23.

- kontroliuojant ir valdant įėjimą į valstybines organizacijas, patalpas ir uždaras teritorijas (oro uostai, jūrų uostai, karinės bazės, elektrinės, naftos perdirbimo įmonės, specialios paskirties įmonės ir kt.).

Pagal Tarptautinės biometrijos grupės (angl. *International Biometric Group – IBG*) biometrinių technologijų rinkos vystymosi prognozę, nuo 2009 m. iki 2014 m. pasaulinės biometrinių sistemų rinkos dydis išaugs 2,7 kartų, t.y nuo 3,4 mlrd. USD iki 9,4 mlrd. USD (žr. 2 pav.)[12].

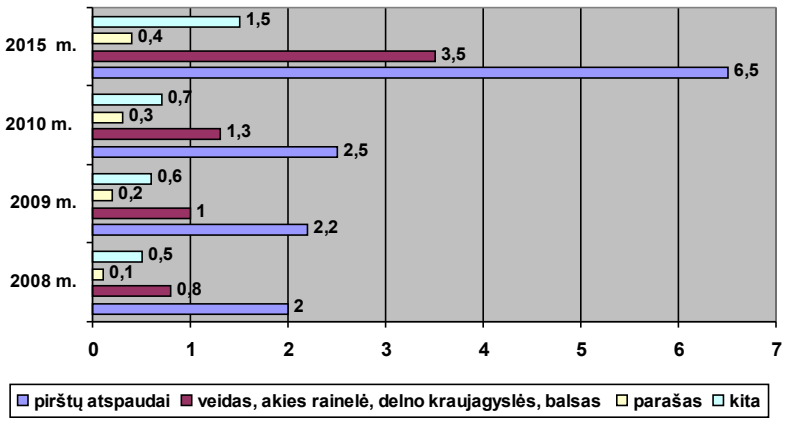


Šaltinis: http://www.axistech.com/WebPages/biometricexactedgrowth.aspx

2 pav. Pasaulinės biometrinių sistemų rinkos vystymosi prognozė (JAV doleriais)

Pasak analitikų, iki 2015 m. smarkiai išaugs biometrinių sistemų, paremtų asmens atpažinimo pagal pirštų atspaudus metodu, panaudojimas viešajame, ypač teisėsaugos srityje, bei privačiame sektoriuose. Išaugs ir kitais metodais paremtų biometrinių sistemų panaudojimo poreikis. (žr. 3 pav.).

[12] Expected Growth. 2008 // http://www.axistech.com/WebPages/biometricexactedgrowth.aspx; prisijungimo laikas: 2011-11-20.



Šaltinis: http://www.prweb.com/releases/2007/04/prweb516626.htm

3 pav. Įvairių biometrinių metodų vystymosi prognozė JAV rinkoje (mln. JAV doleriais)

Pasaulyje šiuo metu yra naudojamos ir toliau tobulinamos įvairiais asmens atpažinimo metodais paremtos biometrinės sistemos, ypač Japonijoje, Rusijoje, JAV. Biometrinių technologijų įmonės veikia šalies ribose arba jungiasi į stambias ir jų veikla plinta po visą pasaulį. Japonijoje biometrines sistemas kuria ir gamina įmonės: *Ayonix Inc., Electric Industry Co., Fujitsu, Sony, Sanyo Electric Co., Secure Design KK, Panasonic, Oki Hitachi Ltd.,* ir kt. JAV – *Iridian Technologies Inc., Visionics Facelt, Eyedentify, Lone Wolf Software, Recognition Systems, Identix Inc., Cross Match Technologies, BioMet Partners Inc., Compaq, SecuGen, Bayometric Inc., DigitalPersona Inc., AOptix, SRI International* ir kt. Rusijoje – *BioLink, Speech Technology Center, Sonda, Elsys, Identification Technologies Company, Artec Group, Vocord, ITV* ir kt.[13]

Europos Sąjungoje (toliau ES) biometrinės sistemos taip pat plačiai naudojamos daugelyje šalių, ypač Didžiojoje Britanijoje. Iš stambesnių įmonių, kuriančių ir gaminančių biometrines sistemas Didžiojoje Britanijoje, galima paminėti: *Arinc, TDSi, Accenture, Acustek Ltd., Aurora Compiuter Services Ltd., Banknote Watch, Biolock UK Ltd., Delaney Secure Ltd., FingerPIN Limited, FingerTec, Ievo, Kingston Biometrics, Trace Tag International* ir kt.[14]

[13] http://findbiometrics.com/companies/; prisijungimo laikas: 2013-04-02.
[14] Ten pat.

1.2. Pagrindiniai asmens tapatybės nustatymo metodai naudojami biometrinėse sistemose

Atsižvelgiant į reikalavimus keliamus visuomenės saugumui (pvz., informacijos apsaugai, valdymo įrenginiams, kai turi būti užtikrinta prieinamumo prie informacijos kontrolė, leidimo ribojimas ir uždraudimas), nusikaltimo vietoje paliktus *pėdsakus ir žymes* ir pan., asmens tapatybės nustatymui plačiai naudojami unikalūs žmogaus kūno požymiai, kuriuos sąlyginai galima būtų skirstyti į dvi grupes.

Pirmajai grupei priskiriami fiziniai ir fiziologiniai žmogaus kūno požymiai:

- rankų pėdsakai – delno, pirštų papiliariniai raštai;
- veninių kraujagyslių sistema (išsidėstymas) išoriniame delno paviršiuje;
- kraujagyslių schema plaštakoje;
- plaštakos geometrija;
- akies rainelės ir tinklainės piešinys;
- veido bruožai;
- veido termograma;
- ausies geometrija;
- kūno kvapas;
- genetinio kodo fragmentai.

Antrajai grupei priskiriami individualaus elgesio požymiai ir charakteristikos:

- rašto rašymo forma ir atlikimo būdas;
- darbo su klaviatūra charakteristika;
- balso parametrai;
- eisena.

Kaip buvo minėta anksčiau, asmuo gali būti atpažintas naudojant biometrines sistemas pagal *fizinius, fiziologinius požymius* ir pagal *elgseną.* Taip pat svarbu paminėti ir sparčiai tobulėjantį *psichologinį metodą,* kuris apima reagavimo į konkrečias situacijas vertinimą arba specialios paskirties bandymus, leidžiančius nustatyti psichologinio profilio atitiktį[15]. Populiariausi metodai, siekiant atpažinti asmenį naudojant biometrines sistemas pagal fizinius ir fiziologinius požymius, yra: atpažinimas pagal pirštų papiliarinį raštą; pagal veido požymius; pagal plaštakos geometriją; pagal kraujagyslių schemą plaštakoje; pagal akies rainelės piešinį; pagal akies tinklainės piešinį. Yra

[15] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. 29 straipsnio darbo grupė. 2012 m. balandžio 27 d. P. 4. // http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm; prisijungimo laikas: 2012-12-20.

ir kitų, mažiau naudojamų, metodų asmeniui atpažinti, pvz., atpažinimas pagal genetinio kodo fragmentą (toliau DNR[16]), ausies geometriją, kūno kvapą ir kt. Labiausiai besiskiriantys ir pasižymintys savo unikalumu yra DNR, akies tinklainės, rainelės ir pirštų atspaudų žmogaus biometriniai požymiai[17].

Populiariausi metodai, siekiant atpažinti asmenį pagal jo elgseną, yra: atpažinimas pagal balso parametrus; pagal asmens pasirašymo būdą; pagal klaviatūros paspaudimo parametrus[18].

Prognozuojama, kad iki 2017 m. ženkliai padidės biometrinių asmens tapatybės nustatymo pagal akies rainelę sistemų naudojimas, nes tokios sistemos jau dabar atpigo, yra labai patikimos ir leidžia atpažinti per atstumą net judantį žmogų. Atitinkamai sumažės biometrinių asmens tapatybės nustatymo pagal pirštų atspaudus sistemų paklausa (žr. 1 lentelę).

1 lentelė. Įvairių biometrinių metodų pasiskirstymo pasaulinėje rinkoje prognozė (procentais)

Biometrinis metodas (požymis)	2009 m.	2017 m.	Skirtumas
Piršto atspaudai	70,13	52,15	-17,98
Veido požymiai	13,66	14,29	0,63
Akies rainelės piešinys	7,98	18,78	10,8
Kraujagyslių schema plaštakoje	2,67	5,77	3,1
Plaštakos geometrija	2,18	5,49	3,31
Balso parametrai	2,15	0	-2,15
Pasirašymo būdas	0,67	1,57	0,9
Kita	0,56	1,96	1,4

Šaltinis: http://www.acuity-mi.com/FOB_Report.php

Atsižvelgiant į greitą technikos evoliuciją ir saugumo sumetimais, kuriamos biometrinės sistemos, kuriose naudojami du ar daugiau metodų asmeniui atpažinti pagal jo biometrinius požymius, pvz., sujungiant veido atpažinimą ir balso registravimą[19]. Įvairiuose šaltiniuose tokios biometrinės sistemos vadinamos *multimodalinėmis biometrinėmis* (angl. *Multimodal biometrics*) arba *multibiometrinėmis* (angl. *Multibiometrics*), mes vartosime žodžių junginį *,,daugiarūšės*

[16] DNR deoksiribonukleino rūgštis. Tai svarbiausia genetinė medžiaga, kuri kontroliuoja paveldimumą. Yra dviejose apvijose, susisukusiose į dvigubą spiralę. Sudaro individualias chromosomas. Žr. http://www.vuoi.lt/index.php?1408667000; prisijungimo laikas: 2012-10-26.

[17] Darbinis dokumentas dėl biometrinių duomenų 12168/02/EN WP 80. P. 3. // ten pat.

[18] Jain A. K. Biometrics: Personal Identification in Networked Society // Kluwer Academic Publishers, 1999. P. 347.

[19] Gricukas G. Biometrija: iš naujo apie naudą ir patikimumą. 2008 //http://www.technologijos.lt/n/technologijos/technologiju_rinka/straipsnis?name=straipsnis-5833; prisijungimo laikas: 2011-11-20.

biometrinės sistemos"[20]. Asmeniui atpažinti gali būti naudojamas ir, pvz., trys skirtingi metodai sujungti sistemoje vienu metu: ką individas žino (PIN kodas, slaptažodis), ką individas turi (atpažinimo kortelė) ir kas individas yra (biometrinis duomuo, pvz., piršto atspaudas). Toks kompleksinis asmens atpažinimo metodų naudojimas didina biometrinės sistemos efektyvumą, tikslumą ir padeda išvengti klaidų[21].

1.3. Biometrinių asmens tapatybės nustatymo sistemų veikimo principas. Tikslumo, efektyvumo vertinimas

Biometrinės sistemos leidžia automatiškai nustatyti asmens tapatybę ir *identifikuoti, verifikuoti* asmenį[22]. Teisėsaugos srityje biometrinės sistemos gali spręsti *paieškos sąrašo analizės uždavinį,* atsakant į klausimą, ar asmuo yra stebimų arba paieškomų asmenų sąraše[23].

Identifikavimas – tai asmens, kurio duomenys saugomi biometrinės sistemos duomenų bazėje, tapatybės nustatymas. Sistema sulygina pateiktą atpažinti biometrinį požymį su daugelio kitų asmenų biometriniais požymiais, esančiais sistemos duomenų bazėse, atsakydama į klausimą: „Kas yra sistemai pristatytas atpažinti asmuo?"[24].

Verifikavimas – tai asmens tapatybės nustatymas, kai asmens pateikiamus biometrinius požymius biometrinė sistema sulygina tik su vieno asmens biometriniais požymiais, esančiais sistemos duomenų bazėse. Biometrinė sistema priima sprendimą, ar pateiktas atpažinti asmuo yra tas pats, kuriuo jis prisistato ir kurio duomenys yra saugomi duomenų bazėse[25].

Asmens atpažinimo procesas pagal jo biometrinius požymius turi bendrą teorinį veiklos modelį: informacijos surinkimas ir įtraukimas į biometrinės sistemos sąrašą, šablono (arba modelio) saugojimas ir informacijos lyginimas[26].

Asmens atpažinimo proceso paruošiamieji žingsniai biometrinėje sistemoje yra:

1. Biometrinių požymių nuskaitymas specialiais įrenginiais;
2. Biometrinių požymių apdorojimas, biometrinio šablono sudarymas;

---

[20] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193 // ten pat.

[21] Ten pat.

[22] Cavoukian A., Stoianov A. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy. 2007 // http://www.ipc.on.ca/images/resources/bio-encryp.pdf; prisijungimo laikas: 2012-10-17.

[23] Stupak V., Vasiliauskas R. Biometrinių autentifikavimo sistemų nagrinėjimo informatikos studijose aspektai // Policijos pareigūnų profesinio rengimo aktualijos. Mokslinių staipsnių rinkinys. – Kaunas: Mykolo Romerio universiteto Viešojo saugumo fakultetas, 2007. P. 82.

[24] Ten pat, P. 83.

[25] Ten pat.

[26] Stan Z. Li, Jain A.K. Enciplopedia of biometrics. – Springer, 2009. P. 192-195.

3. Biometrinio šablono išsaugojimas duomenų saugykloje, susiejant jį su asmeniu[27].

Asmens atpažinimo žingsniai biometrinėje sistemoje yra:

1. Biometrinių požymių nuskaitymas specialiais įrenginiais;
2. Biometrinių požymių apdorojimas, biometrinio šablono sudarymas;
3. Naujai gauto biometrinio šablono palyginamas su anksčiau duomenų saugykloje išsaugotu šablonu;
4. Abiejų biometrinių šablonų atitikimo vienas kitam apskaičiavimas;
5. Įrašo apie atpažinimo arba neatpažinimo faktą išsaugojimas duomenų bazėje[28].

. Biometriniai šablonai (modeliai) gali būti saugomi biometrinės sistemos atmintyje, centrinėje duomenų bazėje, plastikinėse kortelėse, optinėse kortelėse ar mikroprocesorinėse kortelėse[29].

Naudojant biometrines sistemas, gali būti sudėtinga gauti visiškai patikimus rezultatus. Taip gali atsitikti dėl skirtingų aplinkos sąlygų gaunant duomenis (pvz., skirtingas apšvietimas, oro temperatūra) ir skirtingos naudojamos įrangos (pvz., vaizdo kameros, nuskaitymo prietaisai). Praktikoje biometrinės sistemos veiklos rezultatams įvertinti dažniausiai naudojami klaidingos atitikties koeficientas (angl. *False accept rate (FAR*)) ir klaidingos neatitikties koeficientas (angl. *False reject rate (FRR*)). „*Tinkamai suderinus sistemą ir pakoregavus jos parametrus, biometrinių sistemų kritinių klaidų skaičių galima sumažinti iki naudojimui leistino lygio, tai galima padaryti sumažinus klaidingų vertinimų pavojų. Idealioje sistemoje klaidingos atitikties ir klaidingos neatitikties koeficientai būtų lygūs nuliui, tačiau dažniausiai jų tarpusavio santykis yra neigiamas. Dėl didesnio klaidingos atitikties koeficiento dažnai sumažėja klaidingos neatitikties koeficientas*” [30].

Kitaip tariant, biometrinių sistemų tikslumas apibrėžiamas trimis vertėmis:

1. Neteisingo priėmimo galimybe FAR[31];
2. Neteisingo atmetimo galimybe FRR[32];

---

[27] Venčkauskas A., Toldinas J. Kompiuterių ir operacinių sistemų sauga: mokomoji knyga. – Kaunas: Kauno technologijos universitetas, 2008. P. 200.

[28] Ten pat.

[29] Darbinis dokumentas dėl biometrinių duomenų 12168/02/EN WP 80. P. 4. // ten pat.

[30] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 6. // ten pat.

[31] Neteisingo priėmimo galimybė (angl. *False Acceptance Rate (FAR*)) – „tikimybė, kad biometrinė sistema svetimą žmogų atpažins kaip savą. 0,0001 proc. rodo, kad vieną žmogų iš milijono sistema gali atpažinti, nors jo piršto atspaudo duomenų bazėje nėra. FAR turi būti kuo mažesnė, ypač tuo atveju, jei biometriniai skaitytuvai pasikliauja tik vieno tipo asmenybės patvirtinimu ir nereikalauja papildomai įvesti kodo ar pateikti kortelės.”. (Jonaitis A. Akys nemeluoja, pirštai garantuoja. 2007 // http://www.elektronika.lt/straipsniai/pazintiniai/9714/akys-nemeluoja-pirstai-garantuoja;prisijungimo laikas: 2011-11-17).

[32] Neteisingo atmetimo galimybė (angl. *False Rejection Rate (FRR))* – „tikimybė, reiškia kad registruotas vartotojas bus neatpažintas ir reikės dar kartą nuskaityti asmens duomenis...Reiktų atskirti neteisingą atmetimą nuo nesugebėjimo į sistemą įvesti duomenis. Jei dažnai maišomi ar net laikomi vienu. Nesugebėjimu įvesti duomenis laikoma, kai sistemai nepateikiama pakankamai biometrijos informacijos. Tai gali nutikti, pvz., atsiradus purvui ant piršto antspaudų

3. Bendra klaidos galimybe EER[33].

Nei FAR, nei FRR verčių atskirai nepakanka sistemai tinkamai apibūdinti, todėl siūloma remtis EER duomenimis. Realiomis sąlygomis veikianti sistema turi būti vertinama esant FAR = 0[34] [žr. 1 priedą].

Prieš apsisprendžiant naudoti vieną ar kitą biometrinę sistemą, reikia įvertinti ir jos efektyvumą, t.y. gebėjimo laipsnį nustatytomis sąlygomis tenkinti naudotojo poreikius. Siekiant užtikrinti objekto saugos lygį, reikia apskaičiuoti[35] ne tik biometrinės sistemos efektyvumo rodiklį, bet ir įvertinti:

1. Tikslą, kuriam bus naudojama biometrinė sistema;
2. Saugumo reikalavimus objektui;
3. Biometrinės sistemos duomenų subjektų srauto dydį, jutiklio, skaitytuvo (įrenginio) geometrinį dydį;
4. Asmens tapatybės nustatymo algoritmą, programinį aprūpinimą;
5. Biometrinės sistemos kainą ir jos atsipirkimo laiką;
6. Konkretaus biometrinio požymio (požymių) pasirinkimą konkrečiai biometrinei sistemai;
7. Galimybę integruoti biometrinę sistemą į kitas, jau veikiančias sistemas[36].

Kiekvienam biometriniam metodui yra būdingi bendri kriterijai, įtakojantys efektyvumo rodiklio vertes, tokie kaip universalumas, unikalumas, permanentiškumas, pamatuojamumas, atsparumas aplinkos faktoriams ir klastojimui, tikslumas, socialinis priimtinumas[37] [žr. 2 priedą].

1.4. Biometrinių asmens tapatybės nustatymo sistemų įvairovė

Šaltinių analizė parodė, kad istoriškai biometrines sistemas pirmos pradėjo naudoti teisėsaugos struktūros, o vėliau šių sistemų panaudojimo sritys žymiai išsiplėtė visame pasaulyje ir apėmė daugelį kitų visuomenės gyvenimo sričių: prekybos, finansų, civilinės aviacijos, švietimo,

---

skaitytuvo, nepakankamo apšvietimo esant veido atpažinimui, ar neaiškiai kalbant į balso atpažinimo sistemą". (Žr. Ten pat.)

[33] Bendrą klaidos galimybė (angl. *Equal Error Rate (EER))* – FAR ir FRR verčių „aukso vidurys". Sujungus FAR ir FRR diagramas, EER taške tikimybė būti neteisingai atpažintam ar visai neatpažintam yra vienoda. (Žr. Ten pat).

[34] Jain A. K. Biometrics: Personal Identification in Networked Society // Kluwer Academic Publishers, 1999. P. 347.

[35] Žr. Stupak V., Vasiliauskas R. Biometrinių atpažinimo sistemų efektyvumo nagrinėjimo informatikos studijose aspektai // Policijos pareigūnų profesinio rengimo aktualijos. Mokslinių straipsnių rinkinys. – Kaunas: Mykolo Romerio universiteto Viešojo saugumo fakultetas, 2007. P. 87-88.

[36] Ten pat.

[37] Ten pat, P. 89.

sveikatos apsaugos, informacijos apsaugos, t.y. pradėjo sparčiai vystytis ne tik viešajame[38], bet ir privačiame sektoriuje[39].

Tam tikros biometrinės sistemos pasirinkimas vienoje ar kitoje srityje priklauso, visų pirma, nuo dviejų parametrų: *saugumo* ir būtent šios biometrinės sistemos naudojimo *tikslingumo*[40].

Biometrinių sistemų naudojimas teisėsaugos srityje turi eilę esminių skirtumų[41] nuo kitų šių sistemų panaudojimo sričių: pagal biometrinių duomenų registravimo pobūdį, šių duomenų gavimo būdą, jų saugojimo ir naudojimo būdą ir kt., kas yra griežtai reglamentuojama įstatymais.

Analizuojant šaltinius išsiaiškinome, kad populiariausi metodai asmeniui atpažinti pagal jo biometrinius požymius yra atpažinimas pagal pirštų papiliarinį raštą ir atpažinimas pagal veido požymius visose biometrinių sistemų panaudojimo srityse. Aptarsime tai plačiau.

Asmens atpažinimo pagal pirštų papiliarinį raštą (pagal pirštų atspaudus) metodo pagrindas – papiliarinio piešinio rašto unikalumas ant žmogaus pirštų. Biometrinės sistemos, paremtos šiuo metodu, veikia greitai, tiksliai ir yra paprastos naudoti eiliniam vartotojui. Teisėsaugos tikslais naudojamos automatinės pirštų atspaudų atpažinimo sistemos (pvz., ES tai EURODAC ir Vizų informacinė sistema (toliau VIS))[42] šiandien yra pažangiausios.

Asmens atpažinimo pagal pirštų atspaudus metodas pakankamai ištirtas, nėra brangus ir yra plačiai naudojamas viešajame ir privačiame sektoriuose visame pasaulyje asmenų patikros ir atpažinimo tikslais. Laikoma, kad žmogaus pirštų atspaudai laikui bėgant nesikeičia. Tai nėra asmens privatumą itin pažeidžiantis metodas, tačiau visuomenėje gali būti mažiau priimtinas dėl įprasto ir tradicinio šio metodo naudojimo teisėsaugos srityje, dėl ko asmuo gali pirštų atspaudų paėmimą sieti su įtariamojo vaidmeniu[43]. Autoriaus nuomone, šį stereotipą yra pakankamai sunku pakeisti nesant patikimiems informacijos šaltiniams, kurie būtų aiškūs ir suprantami visuomenės nariams.

---

[38] „Viešasis sektorius tai valstybės teikiamų paslaugų ir galimybių savo piliečiams teikimo forma, kaip viešoji gėrybė". pvz., sveikatos apsauga, švietimas, nacionalinis saugumas ir pan. (Valstybės kontrolės 2011-06-21 konferencijos „Koks turi būti viešasis sektorius?" Mykolo Romerio universiteto Politikos ir vadybos fakulteto Vadybos katedros vedėjos Birutės Mikulskienės pranešimas „Viešasis sektorius XXI amžiuje" // http://www.vkontrole.lt/page.aspx?id=15; prisijungimo laikas: 2012-11-03).

[39] Makarski R. A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security, 2002. P. 46. // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407611; prisijungimo laikas: 2012-10- 03.

[40] Umut Uludag, Secure Biometric Systems. Ph. D. Thesis, 2006. P. 1-18. // http://biometrics.cse.msu.edu/Publications/Thesis/UmutUludag_SecureBiometrics_PhD06.pdf; prisijungimo laikas: 2012-11-02.

[41] Žr., pvz., http://www.biolink.ru/technology/biometric.php; prisijungimo laikas: 2012-10-20.

[42] Sprokkereef A. , De Hert P. Ethical practice in the use of biometric identifiers within the EU // Law, Science and Policy, 2007. Vol. 3. P. 181–201. // http://www.vub.ac.be/LSTS/pub/Dehert/200.pdf; prisijungimo laikas: 2012-12-14.

[43] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 20. // ten pat.

Yra pastebėta, kad ne visų žmonių pirštai gali būti apdorojami informacijai (vaizdui) gauti norint paversti tai šablonu (modeliu)[44], be to, žmogaus piršto papiliarinį raštą lengva pažeisti buityje (pvz., pažeidžiant aštriais daiktais, nudeginant) ir dėl to, gali kilti sunkumų biometriniais skaitytuvais nuskaityti pirštų atspaudus ir atpažinti asmenį.

Nesant tinkamų saugumo priemonių, naudojant šias biometrines sistemas, egzistuoja asmens tapatybės vagysčių rizika, kas gali sukelti žmogui sunkių neigiamų padarinių. Tokia rizika yra labai nedidelė, nes šiuolaikinės biometrinės sistemos, paremtos asmens atpažinimo pagal pirštų atspaudus metodu, turi papildomas apsaugos priemones (pvz., temperatūros, paspaudimo jėgos jutiklius), kas didina biometrinės sistemos saugumą ir apsaugo nuo įvairių galimai neteisėtų manipuliacijų su pirštų atspaudų skaitytuvu.

Pirštų atspaudų biometrinėse sistemose dažniausiai būtent šablonų (modelių) naudojimas padeda užtikrinti asmens duomenų apsaugą. Tačiau, atsižvelgiant į pačią biometrinę sistemą ar algoritmą, naudojamą šablonui (modeliui) sukurti, gali kilti susiejimo pavojus su kitomis pirštų atspaudų duomenų bazėmis. Centralizuotas biometrinių duomenų saugojimas, visų pirma, didelėse duomenų bazėse, kelia pavojų susijusį su duomenų *saugumu, susiejamumu* ir *funkcijų iškreipimu*, kai pirštų atspaudai gali būti panaudoti ir kitais, nei pirminiais tvarkymą pagrindžiančiais tikslais, nesant tinkamų apsaugos priemonių[45].

Tarp įmonių, kuriančių ir gaminančių biometrines sistemas, paremtas asmens atpažinimo pagal pirštų atspaudus metodu, galima paminėti: *SecuGen* (USB biometrinių duomenų skaitytuvai skirti kompiuteriams, biometrinės spynos, biometrinės sistemos skirtos įmonėms, įstaigoms, organizacijoms ir pan.), *Bayometric Inc.* (pirštų atspaudų skaitytuvai, įėjimo kontrolės biometrinės sistemos, biometrinių sistemų programavimo įrankiai SDK (angl. *Software Development Kit*)), *DigitalPersona Inc.* (USB biometriniai skaitytuvai, SDK), *BioLink* (pirštų atspaudų skaitytuvai, biometriniai prieigos įrenginiai), *Sonda* (pirštų atspaudų skaitytuvai, biometriniai prieigos įrenginiai, SDK) ir kt.

Asmens atpažinimo pagal veido požymius metodas vystėsi, visų pirma, dėl didelių panaudojimo perspektyvų teisėsaugos srityje, ypač kovojant prieš terorizmą. Toks asmens tapatybės nustatymo metodas, naudojamas kaip atpažinimo ir patikros priemonė, yra patikimas, vyksta greitai, o asmens atpažinimas galimas per atstumą[46]. Tačiau galimybė tai daryti be asmens žinios, tam tikrais

[44] Žr., pvz., Jain A. K. and Feng J., Latent Fingerprint Matching. MSU Technical Report, MSU-CSE-09-10, 2009 // http://www.cse.msu.edu/~rossarun/pubs/FengJainRoss_AlteredFingerprint_TechReport09.pdf; prisijungimo laikas: 2013-02-12.

[45] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 22. // ten pat.

[46] Park U., Tong Y., and Jain A. K. Face Recognition with Temporal Invariance: A 3D Aging Model. 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition, Amsterdam, Netherlands, September 2008 //

atvejais, gali sukelti asmens duomenų apsaugos problemas. Asmens atpažinimo pagal veido požymius metodas leidžia nustatyti ne tik asmens tapatybę, bet ir žmogaus emocijas, etninę, tautinę kilmę, t.y. gauti ir daugiau *ypatingų duomenų* apie asmenį, tad tokių biometrinių sistemų naudojimo *proporcingumas* ir *būtinumas* turi būti įvertintas itin kruopščiai. Gali būti dvimatis (2D) arba trimatis (3D), asmens atpažinimo pagal veido požymius, metodas. Pirmasis turi eilę trūkumų, pvz., asmens atpažinimui gali sutrukdyti akiniai, barzda, pasikeitusi šukuosena, mimika arba sistema reikalauja tik frontalinio veido vaizdo ir pan., tačiau šis metodas yra nebrangus.

Trimatis (3D) asmens atpažinimo pagal veido požymius metodas yra žymiai tikslesnis, bet ir brangesnis. Reikia pažymėti, kad šios biometrinės sistemos susilaukia prieštaringo visuomenės vertinimo, nes tokios sistemos dažniausiai minimos oro uostų saugumo kontekste, siekiant atpažinti teroristus. Realiai, kiekvieno keleivio, pereinančio kontrolės punktą, veidas skenuojamas, bet duomenys nėra įsimenami. Tolimesnis asmens stebėjimas kamera tęsiamas tik tuo atveju, jei asmuo yra atpažintas[47].

Veido atpažinimo funkciją galima integruoti į realiuoju laiku vaizdą fiksuojančius įrenginius. Diegiant tokias sistemas masinio susibūrimo vietose: stotyse, oro, jūros uostuose ir pan. – prasiplečia įtariamųjų asmenų paieškos galimybės. Tokių biometrinių sistemų integravimas į stebėjimo kamerų įrengimus viešosiose vietose gali sukelti visuomenės ir žmogaus teisių apsaugos institucijų pasipriešinimą, nes toks šių sistemų naudojimas gali būti teisiškai tinkamai nepagrįstas ir neužtikrintas tokių priemonių *būtinumas* ir *proporcingumas*[48].

Tarp įmonių, kuriančių ir gaminančių biometrines sistemas, paremtas asmens atpažinimo pagal veido požymius metodu, galima paminėti: *Geometrix Inc.* (3D veido skaitytuvai, programinė įranga), *Genex Technologies* (3D veido skaitytuvai, programinė įranga), *Cognitec Systems GmbH* (SDK, 2D kameros), *Bioscrypt* (3D veido skaitytuvai, programinė įranga), *Artec Group* (3D veido skaitytuvai, programinė įranga) ir kt.

Kiti asmens atpažinimo metodai biometrinėse sistemose naudojami rečiau.

Asmens atpažinimo metodas pagal akies rainelės piešinį (pagal akies rainelę) yra aukšto tikslumo, nes akies vyzdį supančio spalvoto audinio žiedo, t.y. rainelės, piešinys yra unikalus ir nesikeičia visą gyvenimą (išskyrus traumas, patologijas ir pan.).

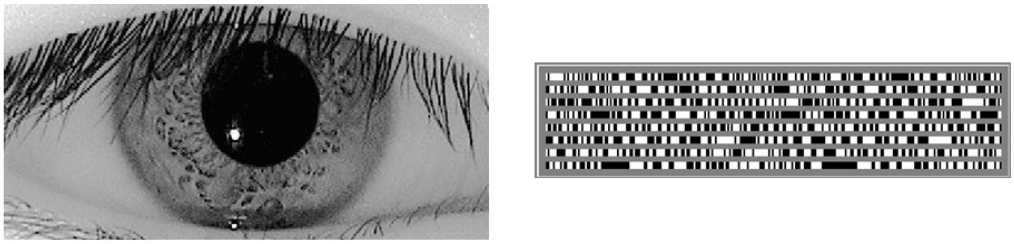
---

http://biometrics.cse.msu.edu/Publications/Face/ParkTongJainTemporalFaceRec_2008.pdf.; prisijungimo laikas: 2011-11-12.

[47] Žr., pvz., Small airports, big problem? 2002 // http://dir.salon.com/story/news/feature/2002/01/08/airport_security/index.html; prisijungimo laikas: 2012-12-13.

[48] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 25. // ten pat.

1987 m. JAV oftalmologai Leonardas Flomas ir Aranas Safiras (*Leonard Flom* ir *Aran Safir*) patentavo savo teiginį, publikuotą 1985 m., kad nėra dviejų tokių pačių akies rainelių ir tai gali būti panaudota asmens identifikavimui. L. Flomas pasiūlė Kembridžo universiteto kompiuterių laboratorijos profesoriui Džonui Daugmanui (*John Daugman*) sukurti algoritmą, skirtą automatiniam asmens identifikavimui pagal akies rainelę. D. Daugman buvo pirmasis, kuris tokį algoritmą sukūrė ir užpatentavo[49] (žr. 4 pav.).



Šaltinis: Introduction to Iris Recognition. http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html

4 pav. Nuskaitytas akies rainelės vaizdas ir jo pagrindu sudarytas biometrinis šablonas

Akies rainelės biometrinių skaitytuvų privalumas yra toks, kad jie nereikalauja asmens koncentracijos į tikslą, akies rainelės vaizdą galima gauti be tiesioginio kontakto su asmens kūnu, o biometrinės informacijos nuskaitymui pakanka net portatyvinės kameros su specializuota programine įranga[50]. Šiandien biometrinės sistemos, paremtos asmens atpažinimo pagal akies rainelę metodu, gali atpažinti ir judantį asmenį. Kai kurių šaltinių[51] duomenimis, asmens atpažinimo pagal akies rainelę metodas, aiškinamas kaip *efektyviausias* ir *tiksliausias* būdas asmeniui atpažinti (išskyrus DNR)[52]. Dar prieš kelis metus tokios biometrinės sistemos buvo brangios, jų paklausa nebuvo itin didelė, tačiau šiai dienai šios biometrinės sistemos atpigo ir, pagal prognozes, iki 2017 m. jų populiarumas ženkliai augs[53].

Tokios biometrinės sistemos yra naudojamos bankomatuose, praėjimo kontrolės punktuose oro uostuose, bankuose, pasienio kontrolės punktuose ir t.t.

---

[49] History of Iris Recognition // http://www.cl.cam.ac.uk/~jgd1000/history.html; prisijungimo laikas: 2013-03-30.

[50] McLaren S. Reliability of iris recognition as a means of identity verification and future impact on transportation worker identification credential. Monterey, California, 2008. P. 11-16. // http://cisr.nps.edu/downloads/theses/08thesis_mclaren.pdf; prisijungimo laikas: 2012-11-15.

[51] Žr., pvz., Daugman J.G. How Iris Recognition Works // IEEE Transactions on Circuits and Systems for Video Technology, 2004. Vol. 14, P. 21-30.

[52] Kranauskas E. Asmens identifikavimas pagal veidą ir akies rainelę. Daktaro disertacijos santrauka. Fiziniai mokslai, informatika (09 p). Vilniaus Universitetas. – Vilnius, 2010. P. 5. // http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2010~D_20100213_102112-81518/DS.005.0.01.ETD; prisijungimo laikas: 2013-01-30.

[53] The Future of Biometrics: 2009 Revised Edition. Market Analysis and Forecasts 2009 to 2017 // http://www.acuity-mi.com/FOB_Report.php; prisijungimo laikas 2013-02-15.

Tarp įmonių, kuriančių ir gaminančių biometrines sistemas, paremtas asmens atpažinimo pagal akies rainelę metodu, galima paminėti: *Iridian Technologies, LG Electronics, Panasonic, OKI* (bendradarbiaujant šioms įmonėms atsirado asmens identifikavimo pagal akies rainelę biometrinės sistemos „Iris Access 2200", „BM-ET500", „OKI IrisPass"), įmones *AOptix, SRI International* ir kt.

Asmens atpažinimo metodas pagal akies tinklainės piešinį (pagal akies tinklainę)[54] – antroji identifikavimo pagal akies parametrus technologija, pagrįsta žmogaus akies dugno kraujagyslių sistemos (tinklainės) identifikacija. Šiuo atveju, akies tinklainės nuskaitymas vykdomas panaudojant mažo intensyvumo infraraudoną šviesą, kuri optinės sistemos (objektyvo) pagalba per akies lęšiuką nukreipiama į akies dugno kraujagyslių sistemą. Sąlyginis šios technologijos trūkumas yra psichologinio pobūdžio – neadekvati žmogaus reakcija į šio biometrinio požymio nuskaitymo procesą (dažniausiai kalbama apie nemalonų pojūtį arba baimę dėl neigiamo poveikio sveikatai). Esmė ta, kad šviesa į tinklainę nukreipiama per objektyvą, kuris turi būti ne toliau kaip per 3 cm. nuo akies išorinio paviršiaus, o žmogaus žvilgsnis turi būti fokusuojamas į nutolusį šviesos tašką. Jeigu žmogaus akis yra pažeista kataraktos, gaunama blogesnė nuskaityto vaizdo kokybė. Atsiranda galimybė, kad nuskaitytas vaizdas bus klaidingai transformuojamas į skaitmeninį kodą, kuris įvedamas į sistemos duomenų bazę. Šio tipo biometrinės sistemos, nepaisant kai kurių sąlyginių apribojimų, yra plačiai naudojamos ypatingo slaptumo prieigos leidimo kontrolės sistemose, kadangi užtikrina patį aukščiausią prieinamumo ribojimą neįregistruotiems vartotojams. Šis metodas yra labai aukšto tikslumo, tačiau brangus.

Tokių sistemų kūrime specializuojasi įmonės *Iridian Technologies Inc., Visionics Facelt, Eyedentifyn* (sukūrusi biometrinę sistemą „Icam 2001"), *Panasonic (CIS) OY* ir kt.

Asmens atpažinimo metodas pagal rankos plaštakos geometriją taip pat patikimas. Nors ši žmogaus biometrinė charakteristika nėra tokia unikali, kaip, pvz., piršto atspaudas, identifikacija pagal rankos plaštakos geometrinius parametrus yra tokia pat patikima, kaip ir daktiloskopinė[55].

Asmens tapatybės nustatymo metodo pagal rankos plaštakos geometriją komercializacijos pradžia laikoma 1974 m., kai JAV mokslininkas Deivydas Šidlauskas (*David Sidlauskas*) užpatentavo trimatį rankos geometrijos identifikavimo įrenginį[56]. JAV kariuomenė apie 1984 m. atliko asmens atpažinimo pagal rankos geometrijos požymius bandymus, taikant juos

---

[54] Spinella E. Biometric Scanning Technologies: Finger, Facial and Retinal Scanning. SANS GSEC, San Francisco, 2003. P. 8-10.

[55] Darma Putra I., Sentosa M. A. Hand Geometry Verification based on Chain Code and Dynamic Time Warping // International Journal of Computer Applications (0975 – 8887). Vol. 38–No.12, 2012. P. 17.

[56] Hand..geometry. 2008 //http://www.sebio.com/showroom/model/T0173/templateCustomWebPage.do?customWebPageId=1226685783487&webId=1225907972827&editCurrentLanguage=1225907972845; prisijungimo laikas: 2013-03-30.

bankininkystėje. Metodo esmė – plaštakos profilio (delno geometrinių parametrų, pirštų, jų ilgio, storio) nuskaitymas. Pirmuosius plaštakos skaitytuvus ID – 3D sukūrė JAV įmonė *Recognition Systems Inc*. Plaštaka, patalpinta specializuotame terminale, skenuojama infraraudona šviesa, o gauta informacija registruojama ir apdorojama. Specialios kompiuterinės programos skaitmeninio kodo pavidalu įvedamos į sistemos atmintį. Čia gauta informacija yra palyginama su duomenų bazėje esančia informacija[57]. Pagrindinis metodo trūkumas – įrenginių dydis (žr. 5 pav.).

Šaltinis: http://recogsys.com

5 pav. Plaštakos skaitytuvas

Tokių ir panašių biometrinių sistemų kūrimo ir gamybos srityje pasaulyje pirmauja įmonės: *Lone Wolf Software, Iridian Technologies Inc., Recognition Systems Inc., Identix Inc., Cross Match Technologies, BioMet Partners Inc.* (pvz., įrenginiai „FingerFoto", „VeryFast", „BioSmart+"), *Identification Technologies Company* ir kt.

Šiandien tokios biometrinės sistemos naudojamos oro uostų kontrolės punktuose keleiviams identifikuoti, ikimokyklinėse įstaigose tėvams identifikuoti, bankininkystėje ir pan. Šis asmens atpažinimo metodas, kaip ir kiti, dažnai jungiamas su kitais metodais daugiarūšėse biometrinėse sistemose.

Asmens tapatybės nustatymui gali būti panaudoti ir tokie unikalūs plaštakos fiziologiniai parametrai, kaip **veninių kraujagyslių sistema (išsidėstymas) išoriniame delno paviršiuje**. Tokio asmens atpažinimo metodo pagrindinis privalumas yra toks, kad asmuo nekontaktuoja su biometriniu skaitytuvu, kas leidžia daryti prielaidą – be asmens žinios, tokių biometrinių duomenų surinkti negalima. Antra, šis metodas yra pigesnis ir tikslesnis negu pastarasis.

2004 m. pradžioje kompanijos *Fujitsu* (Japonija) mokslininkai užpatentavo metodą, kurio esmė – plaštakos ar pirštо peršvietimas šviesa. Šios šviesos bangos ilgis artimas infraraudonai. Gali būti panaudoti keli šviesos šaltiniai ir įvairūs kraujagyslių piešinio vaizdo atstatymo būdai. Įrenginys

[57] Žr., pvz., http://recogsys.com/index.shtml; prisijungimo laikas: 2013-03-30.

formuoja komandas, kurias turi atlikti žmogus (pakelti – nuleisti, sulenkti – ištiesti ranką ir pan.). Tokiu būdu galima gauti visą seriją atitinkamų vaizdų. Gauti vaizdai apdorojami specialia programa, įvedami į atmintį ir sulyginami su joje esančia informacija. Sistema užtikrina aukštą identifikacijos patikimumą. Tokias biometrines sistemas siūloma naudoti bankuose, įėjimo kontrolei užtikrinti į fizines, virtualias zonas ir t.t.[58]

Tarp įmonių, kuriančių ir gaminančių tokias biometrines sistemas, galima paminėti: *Fujitsu, Veid Pte. Ltd.* (biometriniai skaitytuvai, programinė įranga), *Hitachi VeinID* (biometriniai skaitytuvai) ir kt.

Asmens atpažinimo pagal balso parametrus (pagal balsą) metodu[59] paremtos biometrinės sistemos nereikalauja didelių investicijų ir yra pakankamai paprastos. Šis metodas puikiai tinka kriminalistikoje, pvz., asmens tapatybei nustatyti pokalbio telefonu metu. Taip pat šis metodas gali būti taikomas įėjimo kontrolės sistemose, internetinėje prekyboje, lygtinai paleistų iš įkalinimo įstaigų arba nuteistųjų, kuriems bausmės vykdymas atidėtas, asmenų stebėjimo ir kontrolės sistemose, tiriant sukčiavimus, ir t.t.

Tarp įmonių, kuriančių ir gaminančių biometrines sistemas, paremtas asmens atpažinimo pagal balsą metodu, galima paminėti: *Auditech Ltd*., *Nuance, Lernout&Hauspie* ir kt.

Žinoma, yra ir daugiau metodų asmeniui atpažinti, kurie naudojami įvairiose biometrinėse sistemose, tačiau buvo apžvelgti tik labiausiai paplitę. Biometrinės sistemos plačiai naudojamos pasaulio šalyse įvairiose srityse iš kurių gali būti:

- Darbuotojų darbo laiko apskaita bei darbo drausmės gerinimas;
- Moksleivių atsiskaitymas valgyklose;
- Naudojimas, siekiant išvengti alkoholio pardavimo nepilnamečiams;
- Saugumui sustiprinti ir studentų lankomumui patikrinti universitetuose, kitose mokymo, auklėjimo, ugdymo įstaigose;
- Pramogų įstaigų, masinių renginių lankytojų identifikavimas;
- Sporto klubų lankytojų identifikavimas;
- Ligoninių personalo, donorų identifikavimas;
- Civilinės aviacijos lakūnų identifikavimas;
- Identifikavimas bankomatuose ir kt.[60] [žr. 3 priedą]

[58] Palm Secure // http://www.fujitsu.com/us/services/biometrics/palm-vein/; prisijungimo laikas: 2013-04-02.

[59] Каганов А.Ш. Криминалистическая идентификация личности по голосу и звучащей речи. Юрлитинформ. 2009. Т .1. СТ. 3.

[60] Биометрия идет в массы. 2012 // http://www.baltslon.ru/rus/publications/article242/; prisijungimo laikas: 2012-11-03.

Kadangi biometrinių sistemų panaudojimo tikslai gali būti patys įvairiausi, o pamatinis jų panaudojimo tikslas yra, visų pirma, siekis užtikrinti visuomenės saugumą ir viešąją tvarką, pailiustruosime tai keliais atskirais pavyzdžiais.

Labiau išsivysčiusiose ir politiškai stabiliose šalyse, biometrinės sistemos aktyviai naudojamos migracijos kontrolėje. Pvz., jau nuo 2004 m. visi užsieniečiai, besikreipiantys dėl įvažiavimo į JAV, yra tikrinami ir identifikuojami pagal pirštų atspaudus ir veido bruožus („US-Visit" programą)[61]. JAV oro uostuose sėkmingai veikia keleivių lydėjimo programa „Clear" pasinaudojant INSPASS sistema (angl. *Immigration and Naturalization Service passenger accelerated service system*). Šios programos dalyviai gali greitai praeiti kontrolę prieš skrydį, patvirtinę asmens tapatybę pagal pirštų atspaudus ir (arba) pagal akies rainelę. 2012 m. gegužės 23 d. San Francisko oro uosto visuose terminaluose atsidarė nauji punktai su biometrine įranga pagal anksčiau minėtą keleivių lydėjimo programą[62].

JAV policija turi galimybę atpažinti asmenį per atstumą pagal veido bruožus, reikalui esant, papildomai patikrinti pagal kitus požymius – akies tinklainę, pirštų atspaudus, naudojant universalų biometrinį skaitytuvą „Moris". Siunčiant informaciją į nacionalinę duomenų bazę, galima patikrinti ar asmuo paieškomas, ar yra teistas ir t.t.[63]

JAV laisvės atėmimo vietose pirmą kartą nuteistųjų asmenų veido atvaizdas, pirštų ir delno atspaudai įvedami į duomenų bazę, pakartotinai nuteistieji tikrinami pagal minėtus požymius. Planuojama iki 2014 m. papildomai įvedinėti ir saugoti dar vieną nuteistųjų asmenų biometrinį požymį – akies rainelės piešinį. Šios programos pavadinimas „Nuteistųjų identifikavimas ir atpažinimas" (angl. *Inmate Identification and Recognition System IRIS)*[64].

Panašiomis galimybėmis naudojasi visos Lietuvos teisėsaugos institucijos. Policija savo veikloje naudoja daktiloskopavimo įrangą „LiveScan", kuri yra suderinta su automatizuotos daktiloskopinės identifikavimo sistemos „Cogent Systems GmbH AFIS" (toliau CAFIS) duomenų baze. Nuskaitytus kontrolinius rankų pirštų atspaudus, sistema automatiškai siunčia patikrinti į CAFIS, o suformuluotas atsakymas dėl sutapimo arba nesutapimo siunčiamas atgal. Sistemoje galima kaupti ir delnų atspaudus, skaitmeninius veido ir ypatingų žymių atvaizdus[65] (žr. 6 pav.).

---

[61] US-VISIT supports the Department of Homeland Security // http://www.dhs.gov/us-visit-office; prisijungimo laikas: 2013-12-10.

[62] Žr., pvz., http://www.globalsecurity.org/security/systems/inspass.htm; prisijungimo laikas: 2012-11-10.

[63] Amid Privacy Fears, Police Across the Nation Will Roll Out Face-Recognizing iPhone Tech This Year. 2011 // http://www.popsci.com/technology/article/2011-07/amid-privacy-fears-police-across-nation-will-roll-out-face-recognizing-iphone-tech-year; prisijungimo laikas: 2012-11-05.

[64] Eye on crime*:* The FBI is building a database of iris scans, 2012 // http://www.nextgov.com/emerging-tech/2012/06/eye-crime-fbi-building-database-iris-scans/56481/ 2012 11 05; prisijungimo laikas: 2013-01-18.

Šaltinis: http://www.ve.lt/naujienos/kriminalai/policininkai-naudos-moderniausia-elektronine-daktiloskopavimo-iranga-711982/

6 pav. Elektroninis daktiloskopavimo įrenginys „Cogent LiveScan"

2012 m. JAV Federalinis Tyrimų Biuras (toliau FTB) pradeda plėtoti biometrinę sistemą „Sekančios kartos identifikavimas" (angl. *Next Generation Identification*). Tai yra nacionalinė duomenų bazė, kurioje saugomos nuotraukos, akies rainelės vaizdai, balso įrašų pavyzdžiai ir kt., kas padėtų FTB identifikuoti ir surasti nusikaltėlius.

Prancūzijoje taip pat kuriama policijos duomenų bazė nusikaltėliams atpažinti pagal veido bruožus (pvz., iš lauko kamerų vaizdo įrašo padaryto nusikaltimo vietoje). Biometrinė sistema lygins gautus duomenis su linkusių nusikalsti asmenų, teroristų duomeninis, esančiais duomenų bazėje[66].

Atižvelgiant į „arabų pavasario" pasekmes, migracijos kontrolės problema tapo aktualesnė ir ES. 2011 m. buvo paskelbta apie naujos pasienio kontrolės sistemos įvedimą pavadinimu „Užregistruotas keleivis" (angl. *Registered Traveler*), siekiant supaprastini įvažiavimą piliečiams, turintiems biometrinius pasus. Kertant sieną, reikia tik priglausti pasą prie turniketo. Pvz., Ispanijos oro uostuose Madrid-Barajas ir Barcelona-El Prat yra įdiegtos tokios paskirties biometrinės pasienio kontrolės sistemos. Toliau ši sistema taps platesnio masto projekto pavadinimu „Protinga siena" (angl. *Smart Border*) dalimi[67].

Išorės sienų fondo 2010 m. metinės programos vienas iš projekto tikslų buvo sukurti biometrinių duomenų patikros pasienyje sistemą ir aprūpinti pasieniečius įranga, kuria būtų galima sutikrinti trečiųjų šalių piliečių, kertančių ES sieną, vizos numerį su VIS duomenimis, o taip pat

---

[65] Žr. https://www3.cepol.europa.eu/dspace/bitstream/123456789/6752/1/Nedveckis.pdf; prisijungimo laikas: 2012-10-11.

[66] Франция формирует банк данных для автоматической биометрической идентификации. 2011 // http://www.biometrics.ru/news/francija_formiruet_bank_dannih_dlja_avtomaticheskoi_biometricheskoi_identifikacii/01 2 11 05; prisijungimo laikas: 2012-10-11.

[67] EU 'Smart Borders': Commission wants easier access and enhanced security. European Commission - Press release. 2011 // http://europa.eu/rapid/press-release_IP-11-1234_en.htm; prisijungimo laikas: 2012-10-10.

vizos autentiškumą ir jos turėtojo tapatybę. Lietuvoje Valstybės sienos apsaugos tarnybos informacinė sistema (toliau VSATIS), pagal programą, turėjo būti pritaikyta: apdoroti paimtus pirštų atspaudus, juos perduoti į nacionalinę VIS, atvaizduoti kelionės dokumento mikroluste esančią informaciją ir įvertinti dokumento autentiškumą. Taip pat programoje nurodyta, kad „biometrinių duomenų patikros sistema turi veikti visuose pasienio kontrolės punktuose"[68].

2012 birželio 25 d. Valstybinės sienos apsaugos tarnyba (toliau VSAT) prie Vidaus reikalų ministerijos (toliau VRM) sėkmingai užbaigė biometrinių duomenų patikros sistemos diegimo projektą. Projekto metu įsigyta ir įdiegta kelionės dokumentų ir pirštų atspaudų nuskaitymo įranga, VSATIS buvo pritaikyta dirbti su biometriniais duomenimis. Tam tikslui buvo įsigyti stacionarūs „Adaptive Recognition Hungary" kelionės dokumentų bei pirštų atspaudų skaitytuvai, mobilūs dokumentų ir pirštų atspaudų nuskaitymo įrangos komplektai, kas leidžia tiksliai, greitai tikrinti ES išorinę sieną kertančių trečiųjų šalių piliečius (žr. 7 pav.).

Šaltinis: http://www.speedyreader.com/crd_techspecs.htm

7 pav. „Adaptive Recognition Hungary" kelionės dokumentų bei pirštų atspaudų skaitytuvas

Minėti skaitytuvai turi sąsajas ne tik su VSATIS ir ES centrine vizų sistema, o taip pat yra galimybė keistis duomenimis su kitų institucijų informacinėmis sistemomis[69].

Aktyvus biometrinių sistemų įdiegimas pasienio kontrolei vyksta ir Didžiojoje Britanijoje. Asmens atpažinimą, pagal veido bruožus ir pirštų atspaudus, turėjo praeiti visi sportininkai, treneriai, lankytojai arba tiesiog turistai, atvykę į Jungtinę karalystę XXX Olimpinių vasaros žaidynių metu, toks sprendimas buvo paaiškintas galimai padidinta terorizmo grėsme

[68] Išorės sienų fondo 2010 . m. metinė programa //http://www.vrm.lt/fileadmin/Padaliniu_failai/ES_paramos_administravimo/ISf/ISF-2010_LT_RUGSEJO_15.doc; prisijungimo laikas: 2012-11-08.

[69] Biometriniu duomenų patikra pasienyje jau veikia. 2012 // http://atea.lt/news/biometriniu-duomenu-patikra-pasienyje-jau-veikia/; prisijungimo laikas: 2012-11-08.

Olimpiados.metu[70]. Būtent po 2005 m. teroristinių atakų Didžiojoje Britanijoje padidėjo visuomenės saugumo kontrolė ir biometrinių sistemų panaudojimas policijos veikloje. Pvz., Londono metropolitene specialios paskirties policijos būrys (angl. *UK's Metropolitan Police Service – MPS*) tikrina įtariamus asmenis mobiliųjų pirštų atspaudų skaitytuvais ir palygina gautus pavyzdžius su esamais nacionalinėje duomenų bazėje IDENT1[71].

Panašiais įrenginiais jau pradėjo naudotis ir Lietuvos policijos pareigūnai. Šiuo metu policijos veikloje yra naudojami dviejų tipų greitojo identifikavimo įrenginiai ,,Cogent Mobile Ident IIIc" (I tipo) ir ,,Cogent Bluechek" (II tipo) asmens tapatybei nustatyti iš kairės ir dešinės rankų smilių. Patikros metu šiais įrenginiais vietoje galima greitai nustatyti ieškomų ar visuomenei grėsmę keliančių asmenų tapatybę[72] (žr. 8 pav.).

Šaltinis: **http://kriminalai.com/atnaujinama-asmens-pirstu-atspaudu-tikrinimo-iranga/**

8 pav. Greitojo identifikavimo įrenginys „Cogent Mobile Ident IIIc"

Kai kurios pasaulio šalys biometrines sistemas naudoja gyventojų apskaitai. Pvz., Argentinoje kuriamas SIBIOS – Federalinė biometrinė atpažinimo sistema saugumui užtikrinti, į kurią palaipsniui bus įtraukti visų gyventojų biometriniai duomenys, įskaitant ir kūdikius. Tokius savo veiksmus bei sprendimus, valdžia aiškina, kaip siekį kovoti su prekyba vaikais[73].

Pagal *Frost & Sullivan* ekspertų prognozes, biometrinių sistemų poreikis artimiausiu metu bus daugiausia migracinės kontrolės srityje. Praėjus pagrindiniai tendencijai – perėjimui prie biometrinių pasų, dabar laukiama plataus automatinių turniketų vartojimo pradžios. Pranašaujamas dar platesnis ir įvairesnis biometrinių sistemų pritaikymas teisėsaugos srityje. Privačiame sektoriuje

[70]Stringer D. Arrests underline security jitters before Games. 2012 // http://www.nbcolympics.com/news-blogs/2012/arrests-underline-security-jitters-before-olympics.html; prisijungimo laikas: 2012-11-01.

[71] Police mobile fingerprinting trial expands. 2008 // http://www.npia.police.uk/en/10652.htm; prisijungimo laikas: 2012-11-05.

[72] Žr. https://www3.cepol.europa.eu/dspace/bitstream/123456789/6752/1/Nedveckis.pdf; prisijungimo laikas: 2012-10-11.

[73]SIBIOS, National ID biometrics in Argentina. 2011 // http://www.godlikeproductions.com/forum1/message1702000/pg1; prisijungimo laikas: 2012-11-01.

biometrinės technologijos vystysis darbo laiko apskaitos srityje, atsiras didesnis apsaugos nuo vagysčių sistemų ir informacijos apsaugos sistemų poreikis[74].

Akivaizdžios ir logiškos ekspertų išvados leidžia sutikti su tokiomis prognozėmis. Aktyvus perėjimas prie biometrinių dokumentų reikalauja tolimesnio ,,istorijos" vystymosi – biometrinių dokumentų skaitytuvų įdiegimo, plataus vartojimo ir naudojimo pasienio kontrolės punktuose visuomenės labui ir saugumui. Privačiame ir viešajame sektoriuose įvairios biometrinės sistemos padės sustiprinti saugumą ir nusikalstamų veikų prevenciją (pvz., sukčiavimų, vagysčių). Teisėsaugos srityje, esant biometrinėms asmens duomenų bazėms, vykstant aktyviam tarptautiniam bendradarbiavimui, kovojant su nusikalstamumu, terorizmu, siekiant užtikrinti visuomenės saugumą ir viešąją tvarką, biometrinių sistemų panaudojimas yra veiksminga priemonė šiems uždaviniams spręsti.

1.5. Biometrinių asmens tapatybės nustatymo sistemų panaudojimo poreikis Lietuvoje

Šiuolaikinėje valstybėje viešosios tvarkos užtikrinimo funkcija yra įstatymų leidžiamosios bei įstatymų vykdomosios valdžios funkcija, kurią vykdydama valstybė įtvirtina pagrindines žmogaus teises ir laisves, garantuoja jų apsaugą, įgyvendina teisinį visuomeninių santykių, kaip viešosios tvarkos sudedamosios dalies, reguliavimą, kuria ir realizuoja programas, skirtas teisėtumui ir teisėtvarkai valstybėje stiprinti, formuoja teisėtvarkos institucijų sistemą, užtikrina jų veiklos materialinį ir organizacinį aprūpinimą[75]. Tad biometrinių sistemų panaudojimo galimybės, užtikrinant visuomenės saugumą ir viešąją tvarką, tiesiogiai priklauso nuo valstybės ir visuomenės interesų bei poreikių.

Visuomenės saugumas yra glaudžiai susijęs su viešosios tvarkos sritimi. ,,Visuomenės saugumas apima visuomeninius santykius, susijusius su pavojingų žmonių sveikatai ir gyvybei pasekmių, atsirandančių dėl žmonių pavojingų veikų ar stichinių nelaimių, likvidavimu ir tokių pasekmių atsiradimo priežasčių pašalinimu"[76], tad ir biometrinių asmens tapatybės nustatymo sistemų panaudojimą, šio darbo kontekste, turime suprasti kaip priemonę šiems pavojams išvengti, sumažinti ir kitaip kontroliuoti.

---

[74] angl. *Frost & Sullivan* – tai ekonomikos, technologijų, pramonės tyrimų duomenų bazė, kurioje yra pasaulio šalių pramonės rinkų tyrimų ataskaitos, analizės, apžvalgos, prognozės, įvairūs statistiniai rodikliai. Žr. http://www.frost.com/prod/servlet/research.pag; prisijungimo laikas: 2012-11-01.

[75] Novikovas A. Viešosios tvarkos, kaip viešojo saugumo sudedamosios dalies, turinio analizė // Verslo ir teisės aktualijos. – Vilnius: Vilniaus teisės ir verslo kolegija, 2008. T. 2. P. 90.

[76] Ten pat, P. 88.

Susiduriant su vis didėjančiu tarpvalstybiniu laisvu asmenų judėjimu, terorizmo ir kitų sunkių nusikaltimų grėsme, turi būti ieškoma patikimų ir veiksmingų metodų asmens tapatybei nustatyti su minimalia žmogiškojo faktoriaus klaidos tikimybe. Tokiu patikimu ir veiksmingu metodu gali būti biometrinių sistemų panaudojimas Lietuvoje jau šiandien. Kadangi technologijos greitai plečiasi – biometrinių sistemų panaudojimas artimiausioje ateityje gali pakeisti slaptažodžius, kodus, parašus ir kasdieniniame gyvenime.

Jau buvo minėta, kad biometrinės sistemos plačiausia naudojamos visose veiklos srityse tose šalyse, kur yra didelė teroristinių išpuolių galimybė. Lietuvoje terorizmo grėsmė nėra didelė, tačiau šių sistemų panaudojimas ne tik teisėsaugos, bet ir kitose srityse, pvz., elektroninės valdžios, komercinėse sistemose, galėtų taip pat padėti užtikrinti nusikalstamų veikų prevenciją, atskleidimą ir tyrimą, tokiu būdu užtikrinant visuomenės saugumą ir viešąją tvarką.

Šiandien biometrinės sistemos atpigo, tapo spartesnės ir nereikalauja tiek investicijų ir kompiuterinių išteklių kaip anksčiau, tačiau Lietuvoje biometrinės sistemos kol kas nėra plačiai naudojamos. Lietuvos rinka gali pasiūlyti vartotojui už prieinamą kainą durų kontrolės skaitytuvus, biometrinius užraktus ir seifus. Įmonės, įstaigos, organizacijos gali įsigyti ir naudotis prieigos kontrolės biometrinio atpažinimo ir darbo laiko apskaitos terminalais, kas nereikalauja daug lėšų.

Lietuvos telekomunikacijų, duomenų perdavimo ir apsaugos bendrovės, atsižvelgdamos į didėjantį apsaugos technologijų poreikį, šalies rinkai siūlė projektus[77], kuriuos galima būtų panaudoti įėjimo kontrolėje, asmenų paieškai masinėse susibūrimo vietose, pvz., dar 2001 m. tarptautinėje parodoje „Infobalt 2001" viena iš Lietuvos bendrovių pristatė biometrinę veidų atpažinimo sistemą, kuri dėl poreikio nebuvimo nesulaukė didelio susidomėjimo mūsų šalyje. Šiandien Lietuvoje viena dažniausiai visuomenės saugumo, teisės pažeidimų prevencijos tikslais naudojamų priemonių yra vaizdo stebėjimo kamerų (CCTV) įrengimas viešosiose vietose, masinio susibūrimo vietose, gatvėse ir t.t. Jungiant asmens atpažinimo pagal veido požymius sistemas su vaizdo stebėjimo sistemomis, prasiplėstų įtariamųjų asmenų paieškos galimybės, o investicijos, jas patobulinti ir naudoti kartu, būtų nedidelės.

Tikriausiai mažai kam žinoma, kad viena iš įmonių[78] Lietuvoje jau dvidešimt du metus kuria pirštų atspaudų, akies rainelės, veido, delno atpažinimo algoritmus, o tokių įmonių, t.y. kuriančių algoritmus, pasaulyje mažiau nei dvidešimt. Tačiau šios įmonės produkcija, orientuota tik į užsienio rinkas, kas atsirado dėl būtinybės, nes Lietuvoje šiai produkcijai rinkos paprasčiausiai nėra.

[77] Žr., pvz., http://archyvas.infobalt.lt/main.php?&i=1123; prisijungimo laikas: 2013-01-22.

[78] Lietuviškos įmonės, užsienyje išgarsėjusios anksčiau nei Lietuvoje. 2010 // http://www.veidas.lt/lietuviskos-imones-uzsienyje-isgarsejusios-anksciau-nei-lietuvoje; prisijungimo laikas: 2013-01-21.

Projektuose šalies ribose ši įmonė nedalyvauja – parduoda technologijas užsienio, taip vadinamosioms įmonėms-integratorėms, kurios lietuvių produktą pritaiko praktikoje. Lietuvoje sukurtos biometrinės technologijos jau iškeliavo į maždaug šimtą šalių iš kurių ir JAV (amerikiečių kariškiai jas panaudojo teroristų duomenų bazei kurti), Didžioji Britanija (jas naudoja kriminalistai, Londono naktiniai klubai[79] ir kt.).

Vilniaus Gedimino technikos universitete Fundamentinių mokslų fakulteto informacinių technologijų saugos mokslo laboratorijos mokslininkai 2013 m. sausį pristatė jų sukurtą biometrinę sistemą[80], nuskaitančią akies rainelės požymius iš maždaug 5 metrų atstumo. Biometrinė sistema sukurta naudojant plataus vartojimo ir viešai prieinamą įrangą, kuri ženkliai sumažina sąnaudas ir leidžia greitai surinkti skaitytuvą, tad ir panaudojimo galimybės gali būti labai plačios.

Lietuvos integruojančios įmonės, kurios sėkmingai kuria ir vykdo didelės apimties projektus (inžinerinius sprendimus) valstybinės reikšmės infrastruktūros objektuose – pasienyje, geležinkelyje, oro uostuose, šalies didmiesčiuose, iš kurių: perimetro ir vaizdo sistemų įdiegimas pasienio kontrolės punktuose, tranzitinių traukinių į Kaliningradą stebėjimo sistema, LR VRM Europos išorinių sienų (Šengeno) telekomunikacijų tinklas, miestų stebėjimo sistemos realiu laiku, miesto gyventojų perspėjimo ir informavimo sistemos[81] ir kt., galėtų sėkmingai diegti biometrines sistemas ir jau esamas kitos paskirties sistemas (pvz., jungti asmens atpažinimo sistemas su vaizdo stebėjimo sistemomis), o tai įmanoma tik esant valstybės interesui ir visuomeniniam poreikiui. Abejotina, kad toks vidinis poreikis atsiras be išorinių veiksnių, pvz., kitų šalių patirties, ES reikalavimų ir teisinės bazės reguliuojančios nagrinėjamą sritį.

Šiandien Lietuvoje biometrinės sistemos yra naudojamos teisėsaugos srityje, pasienio kontrolės punktuose, kitur viešajame sektoriuje – bankuose, valstybės įmonėse, įstaigose, organizacijose praėjimo kontrolei užtikrinti ir prisijungimui prie elektroninių erdvių. Privačiame sektoriuje biometrinės sistemos naudojamos labai retai, tačiau pirštų atspaudų skaitytuvų poreikis jau atsirado. Yra pastebėta, kad Lietuvos rinka biometrines sistemas, kontroliuojančias patekimą į patalpas (paremtas atpažinimo pagal pirštų atspaudus metodu), o kartu ir darbo laiko apskaitą, siūlo įsigyti, visų pirma, kaip patogią priemonę darbo laikui apskaičiuoti[82], kas prieštarauja *proporcingumo* principui, nes ,,turi būti griežtai įvertinamas tvarkomų duomenų būtinumas ir

[79] Ten pat.

[80] Lietuvos mokslininkai išrado judančio žmogaus tapatybės identifikavimo įrenginį. 2013 // http://www.veidas.lt/lietuvos-mokslininkai-israd o-judancio-zmogaus-tapatybes-identifikavimo-irengini; prisijungimo laikas: 2013-02-20.

[81] Žr. http://www.fima.lt/#sprendimai; prisijungimo laikas: 2013-01-21.

[82] Žr., pvz., http://www.raso.lt/biotime-biometrine-sistema-padesianti-jums-kontroliuoti-patekima-i-patalpas-o-kartu-ir-darbo-apskaita-tai-kompleksinis-sprendimas-leidziantis-automatizuoti-iprastas-tabelio-pildymo-operacijas-darbuotoju-atvykimo-bei-isvykimo-laiko-fiksavima-praejimo-kontr; prisijungimo laikas: 2013-02-07.

proporcingumas, taip pat galimybė pasiekti planuojamą tikslą mažiau privatumą ribojančiomis priemonėmis”[83].

Spartus informacijos ir ryšių technologijų vystymasis lemia viešojo ir privataus sektorių modernizavimą, elektroninių paslaugų plėtojimą. Dėl šios priežasties anksčiau ar vėliau biometrinės sistemos bus naudojamos plačiai ir Lietuvoje. Biometrinių sistemų panaudojimas gali tiesiogiai arba netiesiogiai būti susijęs su žmogaus teisėmis, pvz., teise į privatų ir šeimos gyvenimą, asmens duomenų apsaugą, pagarbą žmogaus orumui, nes biometrinių sistemų duomenų bazėse vienu arba kitu būdu yra saugojami asmens duomenys. Taigi, kyla problema – visų pirma, teisės į privatumą ir asmens duomenų apsaugą. Ši problema plačiau bus nagrinėjama kitame skyriuje.

[83] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 8. // ten pat.

2. ASMENS BIOMETRINIŲ DUOMENŲ TVARKYMO TEISINIO REGULIAVIMO PROBLEMOS

2.1. Pagrindinės asmens biometrinių duomenų tvarkymo teisinio reguliavimo problemos Europos Sąjungoje

Asmens duomenų apsauga yra viena iš žmogaus teisių – teisė į privataus gyvenimo neliečiamumą. Asmens duomenų apsauga yra viena iš pagrindinių teisių Europoje[84], kuri turi būti atitinkamai saugoma.

Platus ir nekontroliuojamas asmens biometrinių duomenų naudojimas kelia susirūpinimą dėl žmonių pagrindinių teisių ir laisvių apsaugos, nes biometriniai duomenys ES šiuo metu yra dažnai naudojami automatinio tapatybės nustatymo procedūrose, naudojant biometrines sistemas. Šiame skyriuje nagrinėsime būtinumo pertvarkyti ES duomenų apsaugos reglamentavimo pagrindus problemą.

Įsigaliojus Lisabonos sutarčiai[85], „buvo sudarytos sąlygos sukurti visapusiškus duomenų apsaugos reglamentavimo pagrindus ir užtikrinti aukštą asmens duomenų apsaugos lygį kartu atsižvelgiant į ypatingą policijos ir teisminio bendradarbiavimo baudžiamosiose bylose pobūdį" [86] ir pakeisti ES duomenų apsaugos taisykles, kad jos apimtų asmens duomenų tvarkymą[87] tiek tarpvalstybiniu, tiek nacionaliniu lygmeniu. Taigi, Lisabonos sutartimi buvo panaikinta ankstesnė ES ramsčių struktūra ir nustatytas naujas visapusiškas asmens duomenų apsaugos visose ES politikos srityse teisinis pagrindas[88].

Europos Komisijos 2009-2010 m. komunikatuose buvo išreikštas požiūris, kad ES turi „sukurti išsamią asmens duomenų apsaugos sistemą, kuri apimtų visas ES kompetencijos sritis" ir

---

[84] Ši teisė įtvirtinta Europos Sąjungos pagrindinių teisių chartijos 8 str. 1 d. ir Sutarties dėl Europos Sąjungos veikimo 16 str. 1 d.

[85] Lisabonos sutartį, iš dalies keičiančią Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį, 2007 m. gruodžio 13 d. Portugalijos sostinėje pasirašė dvidešimt septynių valstybių narių atstovai. Ji įsigaliojo 2009 m. gruodžio 1 d., po to, kai ją ratifikavo visos valstybės narės.

[86] Pasiūlymas Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo. COM(2012)010. Aiškinamasis memorandumas. 2012 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:LT:HTML; prisijungimo laikas: 2013-02-16.

[87] Naujai apibrėžti terminai: *„asmens duomenų saugumo pažeidimas", „genetiniai duomenys"* ir *„biometriniai duomenys"*, remiantis Sutarties dėl Europos Sąjungos veikimo (toliau SESV) 87 str. ir Pamatinio sprendimo 2008/977/TVR 2 str. h. p.

[88] Žr. SESV 16 str.

„užtikrinti, kad pagrindinė teisė į duomenų apsaugą būtų nuosekliai taikoma"[89]. Problemos dėl asmens duomenų apsaugos taisyklių trūkumų ir šių taisyklių modernizavimo būtinumas atsiranda dėl spartaus pažangių technologijų vystymosi, tame tarpe ir biometrinių sistemų vystymosi.

2012 m. sausio 25 d. Europos Komisija pateikė teisės aktų paketą dėl ES asmens duomenų apsaugos reformos, aiškindama, jog asmens duomenų apsaugos taisykles reikia modernizuoti atsižvelgiant į technologijų vystymąsi, kurios „*turi būti orientuotos į ateitį ir būti tinkamos skaitmeniniam amžiui. Technologijų pažanga ir globalizacija iš esmės pakeitė duomenų rinkimo ir teisės į informaciją sampratą. 1995 metais išleistą Europos Tarybos ir Parlamento 46-ąją direktyvą 27 šalys narės yra skirtingai įgyvendinusios nacionalinėje teisėje ir todėl jos taikymas visose šalyse skiriasi. Vieningas teisinis reguliavimas panaikins šiuos skirtumus ir mažins administracinę naštą"*[90].

Šiems išsakytiems poreikiams įgyvendinti, buvo pasiūlytas ES asmens duomenų apsaugos reformos teisės aktų projektų paketas [91], kur iš siūlomų pakeitimų labiausiai svarbūs nagrinėjamame darbe yra šie:

1. „Teisės būti pamirštam" (angl. *„A right to be forgotten")* įgyvendinimas, galimybė asmenims saugiau tvarkyti savo duomenis, pvz. elektroninėje erdvėje;
2. Aiškaus, įsisąmoninto asmens sutikimo gavimas duomenų tvarkymui, galimybė atsisakyti nuo duomenų tvarkymo be jokių pasekmių asmens teisėms ir laisvėms;
3. Vieningo ES duomenų apsaugos taisyklių rinkinio sukūrimas;
4. Nacionalinių duomenų apsaugos institucijų sustiprinimas[92].

Šiandien ES svarbiausias galiojantis asmens duomenų apsaugą reglamentuojantis teisės aktas yra Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau Direktyva 95/46/EB**)**, kuri buvo priimta 1995 m. siekiant apsaugoti pagrindinę teisę į duomenų apsaugą ir užtikrinti laisvą asmens duomenų

---

[89] Žr. Dėl Stokholmo programos ir Stokholmo veiksmų plano, Komisijos komunikatas Europos Parlamentui ir Tarybai „Laisvės, saugumo ir teisingumo erdvė piliečių labui", COM(2009) 262 // http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=lt&DosId=198336 ir Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „ Sukurti laisvės, saugumo ir teisingumo erdvę Europos piliečiams", COM(2010) 171 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:LT:PDF; prisijungimo laikas: 2012-10-25.

[90] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Privatumo apsauga glaudžiai susijusiame pasaulyje, Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje", COM(2012) 09 // EUR-Lex - 52012DC0009 - LT. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT; prisijungimo laikas: 2012-10-25.

[91] Žr. Ten pat.

[92] Asmens duomenų apsaugos naujienų biuletenis. 2012 m. sausis-vasaris Nr. 1 (46) // http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/BiulNr1_2012.pdf; prisijungimo laikas: 2012-10-24.

judėjimą tarp valstybių narių. Tačiau toks egzistuojantis teisinis reguliavimas nėra tobulas, aiškus ir konkretus, kadangi šis dokumentas neapima visų klausimų, kurie iškyla tvarkant biometrinius duomenis, o aptariami tik patys reikšmingiausi, kurie nesudaro visumos pasekmių vaizdo. Nors Direktyvos 95/46/EB tikslas yra užtikrinti vienodą duomenų apsaugos lygį ES, tačiau valstybėse narėse galiojančios taisyklės vis dar labai skiriasi[93], o duomenų valdytojai laikosi skirtingų nacionalinės teisės aktų ir reikalavimų.

Direktyva 95/46/EB taikoma visai asmens duomenų tvarkymo veiklai valstybėse narėse, tiek viešajame, tiek privačiame sektoriuose. Tačiau ji netaikoma tvarkant asmens duomenis, „kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį", pvz., policijos ir teisminio bendradarbiavimo baudžiamosiose bylose srityje[94]. Taip pat Direktyva 95/46/EB netaikoma, kai duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine veikla.

2008 m. Direktyva 95/46/EB buvo papildyta priemone, kuri nustatė konkrečias duomenų apsaugos taisykles, taikomas vykdant policijos ir teisminį bendradarbiavimą, t.y Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos (toliau Pamatinis sprendimas 2008/977/TVR). Tačiau ir Pamatinio sprendimo 2008/977/TVR taikymo sritis yra ribota, nes jis taikomas tik tarpvalstybiniam duomenų tvarkymui ir neapima policijos ir teisminių institucijų vien tik nacionaliniu lygmeniu vykdomos duomenų tvarkymo veiklos. Tokiu būdu, nacionalinėje teisėje valstybėms narėms suteikta didelė veiksmų laisvė. Autorius sutinka, kad dėl šios priežasties gali kilti sunkumų atskirti nacionalinio duomenų tvarkymo lygmenį nuo tarpvalstybinio[95] ir reikalingos aiškios ir nuoseklios duomenų apsaugos taisyklės.

Pamatinio sprendimo 2008/977/TVR pagrindiniai trūkumai yra, visų pirma, plati *tikslų apribojimo principo* išimtis. Taip pat nėra nustatyta, kad reikėtų skirti skirtingas duomenų kategorijas pagal jų *tikslumą* ir *patikimumą* ir „faktais pagrįstus duomenis nuo nuomonėmis ir asmeniniu vertinimu pagrįstų duomenų ir, kad reikėtų skirti įvairias duomenų subjektų kategorijas (įtariamieji, nukentėjusieji, liudytojai ir t.t.), numatant specialias su neįtariamais asmenimis susijusiems duomenims taikomas garantijas" [96].

---

[93]Biometrinių duomenų naudojimo apraiškos Europoje. 2008 //http://www.ada.lt/images/cms/File/Biometriniai%20duomenys%20(Galutinis)%2020080618.doc; prisijungimo laikas: 2012-10-19.

[94] Žr. Direktyvos 95/46/EB 3 str. 2 d. pirmą įtrauką.

[95] Žr. COM(2012) 09 // ten pat.

[96] Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje". COM(2010) 609 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:LT:HTML; prisijungimo laikas 2012-11-11.

Pamatiniu sprendimu 2008/977/TVR nėra pakeičiamos įvairios ES lygmeniu priimtos konkrečiai šiam sektoriui skirtos teisėkūros priemonės dėl policijos ir teisminio bendradarbiavimo baudžiamosiose bylose[97], o būtent Europolo, Eurojusto, Šengeno informacinės sistemos ir Muitinės informacinės sistemos veikimas ir kuriose nustatoma speciali duomenų apsaugos tvarka[98].

Europos Tarybos reglamentas Nr. 2252/2004/EB dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų (toliau Reglamentas Nr. 2252/2004/EB) numatė biometrinių pasų įvedimą su veido atvaizdo bei pirštų atspaudų biometrinėmis duomenimis. Europos Parlamentas, ES duomenų apsaugos darbo grupė, ekspertai išreiškė nuomonę rinktis saugesnius biometrinius duomenis, pvz., rankos kontūrą, nes pasirinktieji ,,atskleidžia ypatingą informaciją apie asmenį ir gali būti naudojami kartu su įvairiomis technologijomis"[99], kas yra nesaugu. Pvz., piršto atspaudų duomenys gali nurodyti įvairias genetines anomalijas arba polinkį tam tikroms ligoms, pirštai palieka pėdsaką ir iškyla grėsmė, kad tokie duomenys bus renkami ir saugomi be asmens sutikimo. Veido atvaizdo biometriniai duomenys gali būti naudojami kartu su nuotolinio veido atpažinimo technologija, kuri leidžia identifikuoti asmenį ir sekti jį per atstumą be jo žinios ir sutikimo[100]. Plėtojant biometrines sistemas, yra būtina atsižvelgti į duomenų apsaugos principus, numatytus Direktyvoje 95/46/EB, atkreipiant dėmesį į ,,ypatingą biometrinių duomenų prigimtį, *inter alia*[101] galimybę rinkti biometrinius duomenis be duomenų subjekto žinios ir neva neabejotiną ryšį su individu"[102].

Taigi, biometrinių duomenų saugojimo būdas buvo paliktas valstybių narių diskrecijai, o tokiu atveju, didelę reikšmę turi nacionalinių asmens duomenų apsaugos organizacijų veikla.

2011 m. vasario 25 d. Žmogaus teisių stebėjimo institutas (toliau ŽTSI), prisijungdamas prie aljanso ,,Hands off biometrics", pasirašė kreipimąsi į Europos Tarybą, kuriuo buvo siekiama atkreipti Europos Tarybos dėmesį į biometrinių duomenų naudojimą pažeidžiant *teisę į privatumą*[103]. Biometrinius veido atvaizdo ir pirštų atspaudų duomenis yra siūloma saugoti

---

[97] Žr. Komisijos komunikatas Europos Parlamentui ir Tarybai „Informacijos valdymo laisvės, saugumo ir teisingumo erdvėje apžvalga", COM (2010) 385. EUR-Lex - 52010DC0385 - LT.

[98] Žr. COM (2010) 609 // ten pat.

[99] Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą. Viešas pareiškimas. 2006 // http://www.hrmi.lt/uploaded/PDF%20dokai/Biometriniu%20duomenu%20naudojimas_viesas%20pareiskimas_2006.pdfprisijungimo laikas: 2012-10-19.

[100] Ten pat.

[101] *lot. ,,inter alia"* - tarp viso kito - reiškia, kad žemesnės galios teisės aktuose draudžiama nustatyti tokį teisinį reguliavimą, kuris konkuruotų su nustatytuoju aukštesnės galios teisės aktuose.

[102] Darbinis dokumentas dėl biometrinių duomenų 12168/02/EN WP 80. P. 10. // ten pat.

[103] Pasirašyta peticija į Europos Tarybą dėl biometrinių duomenų naudojimo. 2011 // http://www.hrmi.lt/./naujiena/600/; prisijungimo laikas: 2012-12-14.

bekontakčiuose radijo dažninio atpažinimo RDA lustuose, kurie yra integruoti pasuose ir (arba) tapatybės kortelėse, o ne duomenų bazėse, kaip tai yra daroma Prancūzijoje, Olandijoje, Lietuvoje.

Siekiant pateikti Europai bendras gaires, ypač biometrinių sistemų industrijai, Direktyvos 95/46/EB 29 str. darbo grupė duomenų apsaugai tvarkant asmens duomenis [104] (toliau 29 straipsnio darbo grupė) dar 2003 m. rugpjūčio 1 d. priėmė darbinį dokumentą dėl biometrinių duomenų, kurio tikslas yra prisidėti prie efektyvaus ir vienodo nacionalinių duomenų apsaugos nuostatų, priimtų remiantis Direktyva 95/46/EB, taikymo biometrinėms sistemoms. Tai buvo labai svarbus dokumentas, kuriuo buvo išaiškintos biometrinių sistemų panaudojimo gairės[105].

Kaip jau buvo paminėta anksčiau, greitas biometrinių technologijų vystymasis ir integracija į įvairias visuomenės veiklos sritis, reikalauja pastovaus dėmesio ir kontrolės. 2012 m. balandžio 27 d. 29 straipsnio darbo grupė išreiškė nuomonę [106] dėl biometrinių technologijų vystymosi, kur daugiau dėmesio skyrė konkrečių biometrinių sistemų diegimo pavyzdžiams ir asmens biometrinių duomenų tvarkymo teisinėms problemoms.

Asmens biometriniai duomenys ir jų skaitmeninis perkėlimas į šabloną (modelį), daugeliu atvejų, yra *asmens duomenys*, nes Direktyvos 95/46/EB 2 str. apibrėžia „asmens duomenis" kaip „bet kurią informaciją, susijusią su asmeniu – duomenų subjektu, kurio tapatybė yra nustatyta arba gali būti nustatyta" [107]. Biometrinių duomenų tvarkymas turi būti grindžiamas vienu iš Direktyvos 95/46/EB 7 str. numatytų *teisėtumo principų*. Jei biometrinių duomenų valdytojas teisėtumo pagrindu laiko asmens sutikimą, turi būti laikomasi reikalavimų, nustatytų Direktyvos 95/46/EB 2 str.[108]

Plačiai naudojami, ypač didelei gyventojų daliai, biometriniai duomenys gali būti laikomi, pagal Direktyvą 95/46/EB, *bendruoju identifikatoriumi*. Tokiu atveju, yra taikoma Direktyvos 95/46/EB 8 str. 7 d. ir valstybės narės turi nustatyti tokių duomenų tvarkymo sąlygas[109].

Kai kurie biometriniai duomenys gali būti laikomi *ypatingais*: tai duomenys, atskleidžiantys rasinę ar etninę kilmę, arba duomenys apie žmogaus sveikatą. Pvz., veido atpažinimo biometrinėse sistemose gali būti tvarkomi duomenys, atskleidžiantys rasinę ar etninę kilmę ir tokiais atvejais, be

---

[104] Asmenų apsaugos, susijusios su asmens duomenų tvarkymu, darbo grupė buvo įsteigta vadovaujantis Direktyvos 95/46/EB 29 str. Tai nepriklausomas ES patariamasis organas duomenų apsaugos ir privatumo klausimais. Grupės uždaviniai išdėstyti Direktyvos 95/46/EB 30 str. ir Direktyvos 2002/58/EB 15 str.

[105] Darbinis dokumentas dėl biometrinių duomenų WP 80 . 2003 // ten pat.

[106] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193 // ten pat.

[107] Žr. Darbinis dokumentas dėl biometrinių duomenų WP 80 . 2003 // ten pat.

[108] Žr. Direktyvos 95/46/EB 2 str., 7 str.

[109] Ten pat 8 str. 7 d.

bendrų apsaugos principų, papildomai turi būti taikomos *specialios apsaugos priemonės*, numatytos Direktyvos 95/46/EB 8 str. [110]

Proporcingumo principo laikymasis, pagal Direktyvą 95/46/EB, yra biometrinių duomenų naudojimo šerdis. Taigi, naudojant biometrines sistemas būtinas *proporcingumo* ir *teisėtumo* įvertinimas, atsižvelgiant į asmens pagrindinių teisių ir laisvių apsaugos riziką. *Proporcingumo* kriterijus visada buvo pagrindinis ir nacionalinėse duomenų apsaugos institucijų priimtuose sprendimuose[111] dėl biometrinių duomenų tvarkymo. Biometriniai duomenys gali būti naudojami tik jei jie yra tapatūs, tinkami ir tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti, o tai reikalauja griežto tvarkomų duomenų ne tik *proporcingumo,* bet ir *būtinumo* įvertinimo.

29 straipsnio darbo grupė pritaria biometrinių sistemų, kurios neįsidėmi biometrinių pėdsakų terminalinėje prieigos įrangoje ar nesaugo jų centrinėje duomenų bazėje, naudojimui, nes kitaip yra pakartotinio šių duomenų panaudojimo kitiems tikslams rizika, o taip pat prieigos be įgaliojimo grėsmė ir pavojus duomenų subjektų teisėms ir laisvėms[112].

Duomenų valdytojas, pagal Direktyvos 95/46/EB 17 str., 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 kokio kito neteisėto tvarkymo[113]. Saugumo priemonės turi būti įgyvendinamos, kai biometriniai duomenys yra tvarkomi, saugomi, perduodami, išrenkamos, palyginamos charakteristikos ir pan., o ypač, jei duomenų valdytojas perduoda tokius duomenis internetu. Saugumo priemonės gali būti sudarytos iš, pvz., šablonų (modelių) šifravimo ir šifravimo raktų apsaugos, papildant prieigos kontrolę ir apsaugą, kad virtualiai būtų neįmanoma iš šablonų (modelių) atkurti pradinius duomenis[114].

Privatumo užtikrinimas, projektuojant biometrines sistemas, yra susijęs su visa biometrinių sistemų vertės grandine, nuo gamintojo iki galutinio vartotojo. Biometrinių sistemų gamintojai ir integruotojai *projektuojant* turėtų *laikytis privatumo užtikrinimo principų,* pvz., užtikrinti automatinį pirminių duomenų ištrynimą sukūrus šabloną (modelį), įdiegti papildomas saugumo priemones, tokias kaip galimybę decentralizuoti duomenų bazę. Konkrečiuose biometriniuose

[110] Ten pat, 8 str.

[111] Vienose Europos šalyse biometriniai duomenys laikomi ypatingais duomenimis (pvz., Italijoje, Liuksemburge, Slovėnijoje, Čekijoje), o kitose – ne (pvz., Norvegija, Portugalija, Belgija, nors netgi Belgijoje biometriniai duomenys susiję su asmens sveikata tam tikrais atvejais gali būti priskirti ypatingiems), visur skiriamas didelis dėmesys, kad ši sfera būtų aiškiai reglamentuota. Žr. Olandijos, Prancūzijos,Vokietijos, Italijos ir Graikijos institucijų sprendimus (pvz., http://www.ada.lt/images/cms/File/Biometriniai%20duomenys%20(Galutinis)%2020080618.doc; prisijungimo laikas: 2012-10-19).

[112] Darbinis dokumentas dėl biometrinių duomenų WP 80 . 2003 // ten pat.

[113] Žr. Direktyvos 95/46/EB 17 str.

[114] Ten pat.

skaitytuvuose įdiegiant užšifravimo funkcijas ir jungiklius, apsaugančius nuo neteisėto duomenų gavimo ir klastojimo, garantuojama apsauga nuo neteisėtos prieigos prie biometrinių duomenų[115].

Gamintojai ir integruotojai turėtų garantuoti biometrinės sistemos tam tikro lygio *lankstumą*, užtikrinantį *proporcingumo, tikslų apribojimo, duomenų kiekio mažinimo ir saugumo principų* laikymąsi. 29 straipsnio darbo grupė rekomenduoja biometrines sistemas projektuoti pagal oficialų projektavimo ciklą. Šį projektavimo ciklą sudaro šie etapai:

1. Rizikos analize ir specialiu poveikio privatumui vertinimu pagrįstų konkrečių reikalavimų nustatymas;
2. Projektui keliamų reikalavimų įgyvendinimo aprašymas ir pagrindimas;
3. Funkcinių ir saugumo bandymų patvirtinimas;
4. Galutinio produkto projekto patikra atsižvelgiant į galiojančiuose teisės aktuose nustatytus reikalavimus[116].

Autorius pritaria, kad sparčiai tobulėjant informacinėms technologijoms, būtina sukurti saugią teisinę aplinką, kurioje būtų ginama privataus gyvenimo neliečiamumo teisė, nes, daugėjant automatizuotai tvarkomų asmens duomenų, kyla grėsmė žmogaus privačiam gyvenimui. Šiandien naujoje sudėtingoje skaitmeninėje aplinkoje ES nepakankamai veiksmingai užtikrinama teisė į asmens duomenų apsaugą, todėl asmens duomenų apsaugos reforma yra būtina.

2.2. Pagrindiniai asmens biometrinių duomenų tvarkymo teisinio reglamentavimo aspektai Lietuvos Respublikoje

Lietuvoje egzistuojančių teisės aktų probleminiai aspektai atspindi biometrinių asmens duomenų tvarkymą ir biometrinių sistemų panaudojimą reglamentuojančios ES teisinės bazės problemas, iš kurių pagrindinė, kaip jau buvo minėta, – *grėsmė asmens privatumui*, nes, visų pirma, Direktyva 95/46/EB yra įgyvendinta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (toliau ADTAĮ) .

„Ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis”[117] yra ADTAĮ tikslas, pagal 1 str. 1 d., tad šis nacionalinis teisės aktas būtų pagrindinis taikytinas ir *biometrinių asmens duomenų* tvarkymui. Biometriniai asmens duomenys turi būti tvarkomi tik jeigu

[115] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. P. 30. // ten pat.
[116] Ten pat.
[117] ADTAĮ 1 str. 1. d. // http://www3.lrs.lt/pls/inter3/oldsearch.preps2?a=314801&b=; prisijungimo laikas: 2012-12-02.

tam yra *teisinis pagrindas*, duomenų tvarkymas yra *tinkamas*, *svarbus* ir *neperteklinis* atsižvelgiant į *tikslus*, kuriais duomenys renkami[118].

Santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita – reglamentuoja ADTAĮ 1 str. 2 d. „Įstatymas nustato fizinių asmenų, kaip duomenų subjektų, teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis"[119]. Jeigu asmens duomenis tvarko fizinis asmuo tik asmeniniams poreikiams, nesusijusiems su verslu ar profesija, ADTAĮ nėra taikomas, pvz., jai asmuo įsigyja savo namams nuo vagystės apsaugoti biometrinę spyną arba, tarkim, savo automobiliui apsaugoti biometrinį užraktą ir pan.

Kaip reglamentuoja ADTAĮ 2 str., „bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai" yra laikoma *asmens duomenimis*. Taigi, autoriaus nuomone, *biometriniai asmens duomenys*, būdami fizinio, fiziologinio, psichologinio, pobūdžio asmens požymiais, yra ADTAĮ sąvokos *asmens duomenys* dalis, nes atskirai sąvokos *biometriniai asmens duomenys* ADTAĮ nėra.

Tais atvejais, jei „... duomenys, susiję su fizinio asmens rasine ar etnine kilme, ... sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą"[120], jie yra laikomi *ypatingais duomenimis.* Autoriaus nuomone, ADTAĮ nėra aiškaus vaizdo, kada biometriniai duomenys bus laikomi ypatingais asmens duomenimis, o kada tokiais nėra laikomi ir duomenų valdytojui gali kilti sunkumų tai atskiriant. Biometrinius duomenis, pagal ADTAĮ 5 str., tvarkyti leidžiama tam tikrais atvejais, pagal tam tikrus kriterijus, o jei jie laikomi ypatingais - draudžiama, išskyrus tam tikrus atvejus[121], todėl duomenų valdytojui, duomenų tvarkytojui ir duomenų subjektui gali kilti neaiškumų ir klausimų, kaip taikyti ADTAĮ vienu ir kitu atveju.

Biometriniai duomenys gali būti tvarkomi tik esant *teisėtam pagrindui.* Asmens duomenų tvarkymas laikomas teisėtu tik tuo atveju, jeigu jis atitinka ADTAĮ 3 ir 5 str. reikalavimus[122], kuriuos privalo užtikrinti duomenų valdytojas, tai būtų: 1) asmens duomenys tvarkomi tik esant *apibrėžtam* ir *teisėtam* tikslui; 2) duomenų tvarkymas turi būti *tikslus, sąžiningas ir teisėtas*; 3)

[118] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių. W 193 // ten pat.
[119] ADTAĮ 1 str. 2 d.
[120] Ten pat 2 str. 1 d.
[121] Žr. Ten pat 5 str.
[122] Ten pat 3 str.

būtina asmens duomenų tvarkymo *nuolatinė kontrolė*[123]; 4) turi būti užtikrintas duomenų *tapatumas*, *tinkamumas*, duomenų rinkimo ir saugojimo *proporcingumas*; 5) būtinas *saugojimo termino priklausomumas nuo tikslų*, dėl kurių šie duomenys buvo surinkti ir tvarkomi.

Naudojant biometrines sistemas turi būti įvertintas, visų pirma, tvarkomų asmens biometrinių duomenų *proporcingumas* ir *būtinumas*. Pvz., diegti biometrinę sistemą, paremtą asmens atpažinimo pagal pirštų atspaudus metodu, įėjimo kontrolei užtikrinti į sveikatingumo ir sporto centrą, saugant duomenis centralizuotai, būtų nei proporcinga nei būtina, pilnai pakaktų ir kitų saugumo priemonių (pvz., magnetinių kortelių). Toks biometrinių duomenų naudojimas ir centralizuotas šių duomenų saugojimas gali būti leidžiamas tik ypatingais atvejais, kur viršesnis yra saugumo interesas[124]. Nagrinėjant biometrinės sistemos *proporcingą* taikymą, reikia atsižvelgti į tai, ar sistema yra *būtina* poreikiui tenkinti ir ar nėra pasirenkama vien dėl patogumo arba ekonomiškumo. Privatumo panaikinimas nebus tinkamas, jei toks panaikinimas neatitiks planuojamą gauti naudą. Visada reikia siekti, kad norimas tikslas būtų pasiektas mažiau privatumą ribojančiomis priemonėmis[125].

Jei, tvarkant asmens duomenis, duomenų subjekto *sutikimas yra privalomas*, sutikimas turi būti *laisvas,* o ne priverstinis[126]. Tai reiškia, kad asmuo turi būti visapusiškai informuotas apie jo biometrinių duomenų tvarkymą, kokios yra jo teisės, kiek galioja jo sutikimas, kada jis gali sutikimą atšaukti, kokiu būdu saugomi ir tvarkomi duomenys, kaip galima susipažinti su informacija ir t.t.

Taikant ADTAĮ 5 str., biometrinių sistemų panaudojimas ir biometrinių asmens duomenų tvarkymas yra laikomas teisėtu ir *be duomenų subjekto sutikimo*, pvz., jei duomenų valdytojo interesai yra svarbesni už duomenų subjektų teisę neregistruotis duomenų biometrinėje sistemoje. Tarkim, taikant *proporcingumo* principą, siekiant kontroliuoti įėjimą į cheminę laboratoriją su pavojingais virusais, į atominę elektrinę arba yra reikalinga priemonė turtui ir asmenims apsaugoti, kai yra objektyviomis aplinkybėmis ir dokumentais pagrįstų konkretaus didelio pavojaus įrodymų, *asmens sutikimas neprivalomas*.

Parenkant organizacines ir technines duomenų saugumo priemones, duomenų valdytojai ir duomenų tvarkytojai privalo vadovautis bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms[127], skirtomis apsaugoti asmens duomenims nuo atsitiktinio ar

[123] Asmens duomenys, nuolat atnaujinami, o netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas. Žr. Ten pat.

[124] Žr., pvz., Liuksemburgo patirtį // http://www.ada.lt/images/cms/File/Biometriniai%20duomenys%20(Galutinis)%2020080618.doc; prisijungimo laikas: 2013-02-25.

[125] Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių. WP 193 // ten pat.

[126] ADTAĮ 5 str.

[127] Žr. Asmens duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymą Nr. 1T-71(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo" // Valstybės žinios.

neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo[128]. Taip pat duomenų valdytojas turėtų nustatyti biometrinių duomenų saugojimo terminą bei užtikrinti, kad po pagrįsto duomenų saugojimo laikotarpio duomenys arba, remiantis tokiais duomenimis, sukurti profiliai būtų visiškai ištrinti. Tvarkant asmenų biometrinius duomenis ar jų šablonus (modelius) automatiniu būdu, pagal ADTAĮ 31 str., duomenų valdytojas privalo Vyriausybės nustatyta tvarka pranešti Valstybinei duomenų apsaugos inspekcijai (toliau VDAI), kuri tam tikrais atvejais atlieka išankstinę patikrą[129].

Jau buvo minėta, kad, dėl centralizuoto biometrinių duomenų saugojimo, didėja pavojus šių duomenų naudojimo, siekiant tarpusavyje sujungti įvairias duomenų bazes. Pavojus, kad tokie duomenys bus pakartotinai panaudoti nesuderinamais tikslais, ypač neleistinos prieigos atveju, visada yra. Todėl sistemose, kuriose biometriniai duomenys naudojami siekiant tarpusavyje sujungti įvairias duomenų bazes, turi būti nustatytos papildomos apsaugos priemonės, pasikonsultavus su kompetentinga nacionaline duomenų apsaugos institucija, kurios kontrolė, tokiais atvejais, turėtų būti visokeriopai sustiprinta.

Tvarkant asmens biometrinius duomenis turi būti įvertinama, kokiu būdu gali būti saugomi asmens biometriniai duomenys: biometrinės sistemos įrenginio atmintyje, centrinėje duomenų bazėje ar išorinėje laikmenoje. Kiekvienu atveju, atsižvelgiant į individualų tvarkymo poreikį, reikėtų pasirinkti mažiausiai asmens privatumą ribojančias priemones. VDAĮ laikosi nuomonės, kad asmens duomenų saugumas labiausiai būtų užtikrinamas asmens duomenis saugant išorinėje laikmenoje, pvz., kortelėje[130].

Policijos veikloje[131], siekiant užtikrinti ko efektyvesnį asmenų pirštų atspaudų, DNR pavyzdžių, veido atvaizdų pateikimą į atitinkamas duomenų įskaitas, būtina gauti tam tikro asmens biometrinius duomenis. Ir anksčiau Lietuvos Respublikos policijos veiklos įstatyme pareigūnams buvo suteikta teisė daktiloskopuoti asmenis, o policijos įstaigoms gautus daktiloskopinius duomenis tvarkyti žinybiniame registre, tačiau asmenų, kuriuos galima daktiloskopuoti, kategorijos nebuvo apibrėžtos tiksliai. Ši spraga buvo ištaisyta nuo 2009 m. spalio 22 d. Policijos veiklos įstatymo 18 str. 13 d. pakeitimu, kuris reglamentuoja, kad *,,policijos generalinio komisaro nustatyta tvarka fotografuoti asmenis, kurių tapatybė nenustatyta, bejėgiškos būklės asmenis, neatpažintus lavonus,*

2008, Nr. 135- 5298.

[128] ADTAĮ 3 str. 1 d.

[129] Ten pat, 31 str.

[130] Viešoji konsultacija dėl pirštų atspaudų ir pagal juos sukurtų modelių tvarkymo // http://www.ada.lt/images/cms/File/viesos%20konsultacijos/pirstu_anspaud.pdf; prisijungimo laikas: 2013-02-18.

[131] Žr. Lietuvos Respublikos policijos veiklos įstatymo 6^2 str.

asmenis, kuriems taikomos prevencinio poveikio priemonės pagal Lietuvos Respublikos organizuoto nusikalstamumo užkardymo įstatymą, asmenis, įstatymų ar kitų teisės aktų nustatyta tvarka įrašytus į policijos įskaitas, asmenis, kuriems įteiktas pranešimas apie įtarimą padarius nusikalstamą veiką, laikinai sulaikytus, teistus asmenis, juos matuoti, aprašyti jų išorės požymius, daryti garso ar vaizdo įrašus, imti pirštų atspaudus, ėminius genetiniam tipizavimui ar pavyzdžius lyginamajam tyrimui ir identifikavimui atlikti" [132].

Pagal Policijos veiklos įstatymą 6 ² str., uždaviniams, numatytiems Lietuvos Respublikos policijos veiklos įstatymo 5 str. įgyvendinti[133], būtini duomenys tvarkomi žinybiniuose registruose, informacinėse sistemose, valstybės registruose[134].

2007-02-14 buvo įsteigtas, o 2011-05-01 pradėjo veikti Daktiloskopinių duomenų registras[135]. Žinybinis Lietuvos policijos daktiloskopinių duomenų registras buvo įsteigtas automatizuotos daktiloskopinės identifikacijos sistemos duomenų bazės pagrindu. Daktiloskopinių duomenų registro tvarkymo įstaiga yra Lietuvos policijos kriminalistinių tyrimų centras (toliau KTC), kuris taip pat yra ir DNR registro tvarkymo įstaiga. Pastarasis buvo įsteigtas 2011-01-26, o pradėjo veikti 2011-07-01[136].

KTC keičiasi daktiloskopiniais ir DNR duomenimis pagal *Priumo*[137] ir kitas sutartis, taip pat pagal dvišalius susitarimus. KTC informacinės sistemos yra integruotos į Lietuvos policijos, VRM ir

---

[132] Žr. Lietuvos Respublikos policijos veiklos įstatymo 1, 2, 3, 6^2, 7, 11, 12, 15, 16, 18, 19 straipsnių pakeitimo ir papildymo įstatymą.

[133] Pagal Lietuvos Respublikos policijos veiklos įstatymą 5 str., vienas iš pagrindinių policijos uždavinių yra viešosios tvarkos ir visuomenės saugumo užtikrinimas. Šis uždavinys susijęs su kitais uždaviniais: žmogaus teisių ir laisvių apsauga, neatidėliotinos pagalbos teikimu asmenims, kai ji būtina dėl jų fizinio ar psichinio bejėgiškumo, taip pat asmenims, nukentėjusiems nuo nusikalstamų veikų, kitų teisės pažeidimų, stichinių nelaimių ar panašių veiksnių; nusikalstamų veikų ir kitų teisės pažeidimų prevencija; nusikalstamų veikų ir kitų teisės pažeidimų atskleidimu ir tyrimu; saugaus eismo priežiūra. Visi šie uždaviniai yra vienodai svarbūs ir nėra izoliuoti vienas nuo kito.

[134] Žr. Lietuvos Respublikos policijos veiklos įstatymo 6^2 str.

[135] Į Daktiloskopinį ir DNR žinybinius registrus duomenis teikia Policijos įstaigos; Kalėjimų departamentas prie Lietuvos Respublikos teisingumo ministerijos ir jam pavaldžios įstaigos; Lietuvos Respublikos prokuratūros; Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos; Lietuvos Respublikos specialiųjų tyrimų tarnyba; Lietuvos kariuomenės Karo policija; Lietuvos Respublikos valstybės saugumo departamentas; Finansinių nusikaltimų tyrimo tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos; Lietuvos Respublikos muitinė; Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos; užsienio valstybių teisėsaugos institucijos bei tarptautinės teisėsaugos organizacijos.

[136] Lietuvos policijos generalinio komisaro įsakymas Nr. 5-V- 42 „Dėl DNR duomenų registro steigimo ir nuostatų patvirtinimo" // Valstybės žinios. 2011, Nr.10-475.

[137] 2008 m. Sprendime dėl Priumo sutarties išdėstytos taisyklės, taikomos keitimuisi DNR analitėmis, pirštų atspaudais, transporto priemonių registracijos duomenimis ir informacija apie asmenis, įtariamus rengiant teroristų išpuoliu, siekiama sustiprinti nusikalstamų veikų, visų pirma terorizmo ir tarpvalstybinio nusikalstamumo prevenciją ir užtikrinti viešąją tvarką didelių renginių metu // Tarybos sprendimas 2008/615/TVR, OL L 210, 2008. P. 1; Tarybos sprendimas 2008/616/TVR, OL L 210, 2008. P. 12.

kitų institucijų infrastruktūrą, siunčiami duomenys į Interpol'ą ir EURODAC sistemą. KTC paskirtas įgaliota institucija – nacionaliniu kontaktiniu centru su EURODAC[138].

Tai pat atkreiptinas dėmesys į Lietuvos Respublikos baudžiamojo proceso kodekso 156 str., kuriame yra nustatyta, kad ikiteisminio tyrimo pareigūno ar prokuroro nutarimu, įtariamasis, o teismo nutartimi kaltinamasis, gali būti fotografuojami, filmuojami, matuojami, gali būti paimami jų rankų atspaudai ir pavyzdžiai genetinei daktiloskopijai nepriklausomai nuo įtariamojo, kaltinamojo nesutikimo[139].

Tokiu būdu, ar vykstant baudžiamajam persekiojimui, ar vadovaujantis Policijos veiklos įstatymu, yra galimybė gauti asmens biometrinius duomenis ir įtraukti į policijos žinybinius registrus. Taip, 2013-01-01 dienai, DNR duomenų registre yra 69 056 DNR analitės, 2012 m. yra nustatyti 345 sutapimai. Daktiloskopinių duomenų registre yra 210 232 pirštų atspaudų, 57 656 delnų atspaudų, 20 000 skaitmeninių veido ir ypatingų žymių atvaizdų. Identifikuota 639 asmenų, iš jų 257 naudojant greitojo identifikavimo įrenginius[140]. Neabejotina, kad tokios galimybės, esant sutapimams, padeda išaiškinti daugiau nusikalstamų veikų, atpažinti ir surasti asmenis.

Išduodant ir naudojant Lietuvos Respublikos pilietybę ir (ar) asmens tapatybę patvirtinančius dokumentus, asmens biometriniai duomenys taip pat yra tvarkomi. Tai yra pavyzdys, kai duomenų valdytojas privalo tvarkyti biometrinius duomenis, kad laikytųsi jam nustatytos teisinės prievolės.

Nuo 2006 m. rugpjūčio 28 d. į Lietuvos Respublikos pasus[141] elektroniniu būdu pradėjo įrašinėti asmens biometrinius duomenis, veido atvaizdą, o nuo 2009 m. birželio 29 d. ir asmens pirštų atspaudus[142]. Dar 2006 m. ŽTSI atkreipė dėmesį į tai, kad Lietuvoje, kaip jau buvo minėta anksčiau, visuomenė nebuvo tinkamai informuota apie pasų su biometriniais duomenimis įvedimą. Nei politiniame, nei visuomeniniame lygmenyje nevyko diskusijos dėl šių dokumentų patikimumo, efektyvumo ir, svarbiausia, dėl jų įtakos asmens teisei į privataus gyvenimo gerbimą[143], tad, dėl informacijos stokos ir neimlumo naujovėms, biometrinių sistemų diegimas ir naudojimas gali ilgiau likti nesuprastu, o gal, kai kuriais atvejais, net nepriimtinu dalyku. Tačiau turime suprasti – nuo kada ir kokios apsauginės savybės bei biometrikos standartai turėjo atsirasti ES valstybių narių

---

[138] Lietuvos Kriminalistinio centro veiklos ataskaitos // http://ktc.policija.lt/lt/veikla/planai_ir_ataskaitos.html; prisijungimo laikas: 2011-10-21.

[139] Žr. Lietuvos Respublikos baudžiamojo proceso kodekso 156 str.

[140] LPKTC 2012 m. veiklos ataskaita. 2012 // http://ktc.policija.lt/lt/veikla/planai_ir_ataskaitos.html; prisijungimo laikas: 2013-02-19.

[141] Lietuvos Respublikos paso įstatymas // Valstybės žinios. 2001, Nr. 99-3524; 2006, Nr. 77-2957.

[142] Lietuvos Respublikos pasas // http://www.dokumentai.lt/pasas.php; prisijungimo laikas: 2011-12-15.

[143] Žmogaus teisių stebėjimo instituto 2011 m. veiklos ataskaita. Vilnius, 2012 // http://www.hrmi.lt/uploaded/PDF%20dokai/Ataskaita__ZTSI_GALUTINE_2011_1.pdf; prisijungimo laikas: 2012-10- 24.

pasuose ir kelionės dokumentuose, 2004 m. gruodžio 13 d. nustatė Reglamentas Nr. 444/2009 EB[144], o tai yra ne diskutuotinas, o privalomas teisės aktas.

Kiti dokumentai: Asmens tapatybės kortelė[145], Lietuvos Respublikos tarnybinis pasas[146], Lietuvos Respublikos užsieniečio pasas, Asmens be pilietybės kelionės dokumentas, Pabėgėlio kelionės dokumentas, Leidimas gyventi Lietuvos Respublikoje[147] taip pat sukurti atsižvelgiant į naujausius ES reikalavimus ir Tarptautinės civilinės aviacijos organizacijos (ICAO) rekomendacijas ir nuo 2006 m. į minėtus asmens dokumentus elektroniniu būdu pradedami įrašyti asmens biometriniai duomenys, o nuo 2009 m. ir asmens biometriniai duomenys – pirštų atspaudai[148] .

Lietuvos Respublikos asmens tapatybės kortelės įstatymo 2, 4, 5 str. pakeitimo bei papildymo ir įstatymo papildymo 1^1 str. įstatymas įteisino asmens biometrinių duomenų bei asmens atpažinimo elektroninėje erdvėje sertifikato ir kvalifikuoto sertifikato diegimą į asmens tapatybės korteles.

Asmens biometriniai duomenys saugomi LR gyventojų registre[149], t.y. *centralizuotai.* 29 darbo grupė pažymėjo, kad toks saugojimas gali padidinti neteisėto duomenų panaudojimo ir pasisavinimo pavojų, o taip pat gali padidėti biometrinių identifikatorių naudojimo tikimybė kaip „prieigos raktu" prie įvairių duomenų bazių, taip susiejant duomenų rinkinius[150]. Autorius sutinka, kad yra tokia rizika, kaip ir įsilaužimo į duomenų bazes, programinės įrangos klaidos rizika, o taip pat duomenų klastojimo, naikinimo bei keitimo rizika. „Ši rizika yra ypatingai didelė Lietuvoje, kur žmonių informuotumas ir sąmoningumas duomenų rinkimo, saugojimo ir panaudojimo srityje yra žemas, duomenų registrų sistema yra ypač centralizuota ir saugomi duomenys yra gana nesunkiai

---

[144] 2009 m. gegužės 28 d. Europos Parlamento ir Tarybos reglamente (EB) Nr. 444/2009, iš dalies keičiančiame Tarybos reglamentą (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų, reglamentuota, kad pasuose ir kelionės dokumentuose turi būti labai saugi laikmena, kurioje yra veido atvaizdas. Valstybės narės į sąveikias formas taip pat įtraukia du tiesiai įspaustus pirštų atspaudus. Duomenys turi būti apsaugoti, o laikmena turi būti pakankamos talpos ir galios, kad būtų garantuotas duomenų integralumas, autentiškumas ir konfidencialumas.

[145] Asmens tapatybės kortelės įstatymas // Valstybės žinios. 2001, Nr. 97-3417; 2008, Nr. 76-3007, 2010, Nr. 125-6379.

[146] Lietuvos Respublikos tarnybinio paso įstatymas // Valstybės žinios. 2000, Nr. 7-178; 2006, Nr. 77-2958.

[147] Lietuvos Respublikos „dėl užsieniečių teisinės padėties" įstatymas // Valstybės žinios. 2004, Nr. 73-2539; 2012, Nr. 85-4450.

[148] http://www.dokumentai.lt/viewpage.php?page_id=49#atk 2009; prisijungimo laikas: 2012-10-19.

[149] Lietuvos Respublikos gyventojų registro įstatymas // Valstybės žinios. 1992, Nr. 5-78; 2006, Nr. 65-2387; 2012, Nr. 80-4142.

[150] Nuomonė 3/2005 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. P. 1–6 // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_lt.pdf; prisijungimo laikas: 2013-01-16.

prieinami trečiosioms šalims”[151]. Šios cituotos nuomonės aktualumas nekėlė abejonių iki 2013 m. sausio 1 d., kol neįsigaliojo pakeistas ir papildytas LR gyventojų registro įstatymo 11 str. nauja 5 dalimi, kur yra sukonkretinta ir suformuluota kam gali būti teikiami asmens biometriniai duomenys: *„Veido atvaizdas, pirštų atspaudai ir parašas gali būti teikiami tik teisėtvarkos ir asmens tapatybę patvirtinančius dokumentus išduodančioms institucijoms...valstybės institucijoms juridinę galią turinčių dokumentų gamybai tik esant asmens sutikimui. Veido atvaizdas gali būti teikiamas finansų įstaigoms tik tų asmenų, kuriems ketinama suteikti finansines paslaugas, susijusias su rizikos prisiėmimu. Veido atvaizdas teikiamas sveikatos priežiūros įstaigoms nenustatytos asmens tapatybės pacientų asmens tapatybei patvirtinti ir (ar) nustatyti, taip pat notarams ir antstoliams – teisės aktų nustatytoms funkcijoms atlikti, kai to reikia kaip papildomos asmens identifikavimo priemonės asmens tapatybei nustatyti”*[152], tačiau manytina, kad žmonių informuotumas ir sąmoningumas kam gali būti teikiami jų biometriniai duomenys ir toliau lieka žemas.

Tęsiant biometrinių sistemų panaudojimo priimtinumo problemos temą, pažymėsime, kad nuo pirmųjų biometrinių dokumentų įvedimo dienos iki dabarties situacija šiek tiek pasikeitė, taip, pvz., 2012 m. gruodžio mėnesį Vilniaus Gedimino technikos universitete vykusioje apklausoje „ Biometrinių atsiskaitymų technologijų perspektyvos Lietuvoje”[153] iš 53 apklaustųjų ~ 41 proc., pagrinde minėtos mokymo įstaigos studentų, pareiškė žinantis kas yra biometrija. ~ 90,6 proc. pasisakė, kad norėtų naudotis biometriniais įrenginiais atsiskaitant. ~ 73,6 proc. nurodė, kad priimtiniausias jiems būtų pirštų atspaudų naudojimas tokiuose įrenginiuose. Apklaustieji mano, kad tai padidintų atsiskaitymo greitį, o taip pat įžvelgė kitą privalumą – daugybės kodų nebuvimą. Pamažu tam tikra visuomenės dalis pradeda suprasti, kas yra aplamai biometrinės technologijos, kokia gali būti šių technologijų nauda, tačiau šis procesas vyksta žymiai lėčiau, nei visame pasaulyje.

Biometrinių technologijų naudojimas kelia daug svarbių klausimų. Šie klausimai susiję su biometrinių sistemų panaudojimu viešajame ir privačiame sektoriuje, poveikiu asmens privatumui, biometrinių sistemų veikimo sutrikimais, galimu piktnaudžiavimu biometriniais duomenimis, jų neteisėtu naudojimu. Šiandien skiriamas vis didesnis dėmesys duomenų apsaugos svarbumui. Yra sugriežtinta kontrolė dėl galimai neteisėto asmens duomenų tvarkymo. Pvz., kiekvienas asmuo gali

[151] Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą. Viešas pareiškimas. 2006 // http://www.hrmi.lt/uploaded/PDF%20dokai/Biometriniu%20duomenu%20naudojimas_viesas%20pareiskimas_2006.pdfprisijungimo laikas: 2012-10-19.

[152] Lietuvos Respublikos gyventojų registro įstatymo 7, 9, 11 straipsnių pakeitimo ir papildymo įstatymas // Valstybės žinios. 2012, Nr. 80-4142.

[153] Žr. Biometrinių atsiskaitymų technologijų perspektyvos Lietuvoje // http://apklausa.lt/f/biometriniu-atsiskaitymu-technologijos-perspektyvos-lietuvoje-769j8gh/answers.html?utf8=%E2%9C%93&dur_min=0&dur_max=3481; prisijungimo laikas: 2012-12-09.

kartą per metus nemokamai gauti informaciją, net neišėjęs iš namų[154], ar buvo tvarkomi jo asmens duomenys (pvz., valstybės registruose) ir imtis atitinkamų veiksmų, informacijai gavus, dėl galimai neteisėto tokio domėjimosi. VDAI daugiau dėmesio skiria visuomenės informavimui asmens duomenų tvarkymo klausimais rengdama konferencijas, viešąsias konsultacijas, informacinius biuletenius, pranešimus spaudai ir t.t. Yra parengta ir viešoji konsultacija dėl pirštų atspaudų ir pagal juos sukurtų šablonų (modelių) tvarkymo[155], kurioje išsamiai išaiškinta, kaip taikyti ADTAĮ, naudojant tokias biometrines sistemas. Tačiau tokios informacijos plačiajai visuomenei reikia teikti daugiau, nes dėl informacijos stokos, atsitiktinių, nepatikimų šaltinių gali atsirasti ir iškreiptas visuomenės suvokimas apie biometrinių sistemų panaudojimo principus, tikslus ir t.t.

Teisėsaugos srityje Lietuvoje kai kurių biometrinių sistemų panaudojimas jau tapo kasdienybe, tačiau vis dėl to ši praktika yra naujovė, todėl dar lieka neaiškumų ir klausimų.

Lietuvos Respublikoje galiojantys teisės aktai, susiję su duomenų apsauga, iš esmės atitinka ES teisės aktuose keliamus reikalavimus, tačiau esami įstatymai Lietuvoje, reglamentuojantys asmens duomenų tvarkymą, nebuvo patikrinti biometrinių duomenų kontekste. Taigi, lieka neaišku, kaip problemos dėl biometrinių duomenų tvarkymo būtų sprendžiamos pagal esamą teisinę sistemą. Tokias spragas turėtų užpildyti teismų praktika ir naujasis asmens duomenų apsaugos ES teisinis reglamentavimas, įvykus asmens duomenų apsaugos reformai.

[154] Žr., pvz., Elektroninės valdžios vartai. Paslaugos. http://www.epaslaugos.lt/portal/citizen/popular/services.

[155] Viešoji konsultacija dėl pirštų atspaudų ir pagal juos sukurtų modelių tvarkymo // http://www.ada.lt/images/cms/File/viesos%20konsultacijos/pirstu_anspaud.pdf; prisijungimo laikas: 2013-02-08.

3. BIOMETRINIŲ ASMENS TAPATYBĖS NUSTATYMO SISTEMŲ PANAUDOJIMO GALIMYBIŲ LIETUVOJE VISUOMENINIS VERTINIMAS

3.1. Empirinių duomenų rinkimo metodika

Lietuvoje iki šiol nebuvo atlikta išsamių tyrimų biometrinių sistemų panaudojimo užtikrinant visuomenės saugumą ir viešąją tvarką galimybėms ištirti. Siekiant atskleisti visuomeninį požiūrį ir nuomonę apie biometrinių sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje, buvo parengtas ir atliktas tyrimas.

Tyrimo metu buvo panaudotas anketavimo metodas ir pasirinktos dvi apklausos rūšys:

- anketinė apklausa el. paštu;
- internetinė apklausa.

Kadangi biometrinės sistemos naudojamos kiek viešajame tiek privačiame sektoriuje, buvo priimtas sprendimas, kad imtį sudarys Kriminalinės policijos skyrių pareigūnai, kaip viešojo sektoriaus atstovai[156], o privataus sektoriaus atstovais gali būti bet kurie kiti asmenys.

Daroma prielaida, kad Kriminalinės policijos skyrių pareigūnai naudoja biometrines sistemas bent jau dėl tarnybinės veiklos specifiškumo, todėl šios tiriamos grupės atstovai galimai turi daugiau žinių apie biometrinių sistemų panaudojimo ypatumus, tikslus, galimybes ir pan., atitinkamai kitos tiriamos grupės atstovai tokių žinių turi mažiau arba visai neturi.

Tyrimui atlikti buvo parengtos dviejų rūšių anketos. Viena anketa skirta Kriminalinės policijos skyrių pareigūnams, kita - plačiosios visuomenės nariams [žr. 4 priedą]. Anketoje Kriminalinės policijos skyrių pareigūnams yra 14 uždarų klausimų. Jų anketavimas buvo vykdomas el. paštu. Analogiška anketa, išskyrus klausimus Nr. 3 ir Nr. 14[157], buvo patalpinta plačiajai visuomenei interneto svetainėje www.apklausa.lt.[158]

Vilniaus apskrities vyriausiojo policijos komisariato Vilniaus miesto teritorinių policijos komisariatų visiems Kriminalinės policijos skyrių pareigūnams bei jų vadovams[159] 2012 m. lapkričio pabaigoje – gruodžio pradžioje buvo išsiųstos el. paštu 260 anketos. Gauta atsakymų (užpildytų

[156] Pasirinkti teisėsaugos srities pareigūnai visų pirmą dėl biometrinių sistemų praktinio naudojimo tarnybinėje veikloje ir esant tokio naudojimosi rezultatams.

[157] Žr. 5 priedą, anketos Kriminalinės policijos skyrių tyrėjams ir jų vadovams klausimus Nr. 3 ir Nr. 14.

[158] Anketos nuoroda http://apklausa.lt/f/biometriniu-asmens-tapatybes-nustatymo-sistemu-panaudojimo-galimybes-uztikrin-x12q585/answers/new.html?advertised=true.

[159] Kurių kontaktai buvo patalpinti www.vilnius.policija.lt nurodytu tyrimo atlikimo laikotarpiu.

anketų) – 96, tokio respondentų kiekio statistiškai reikšmingoms išvadoms padaryti pakankamumas yra su ~ 95 proc. tikimybe, ir ~ 8 proc. paklaida[160].

Buvo numatytas analogiškas respondentų skaičius internetinėje svetainėje www.apklausa.lt. Pasiekus reikiamą atsakymų kiekį, tyrimas buvo sustabdytas.

Gavus iš visų respondentų reikiamą atsakymų kiekį, duomenys buvo perkelti į duomenų bylas. Matuojamiesiems požymiams randami absoliutūs, santykiniai bei procentiniai dažniai (matavimo skalės nominalinės, apdorota su ,,Excel"). Gauti duomenys analizuojami, interpretuojami [žr. 5 priedą].

3.2. Visuomenės informuotumas apie biometrinių asmens tapatybės nustatymo sistemų praktinį panaudojimą teisėsaugos srityje

Visuomenės narių informuotumą apie esamų Lietuvoje biometrinių sistemų praktinio panaudojimo privalumus teisėsaugos srityje atskleidė atsakymai į klausimus:

- ✓ *Ar Jums yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos (ADIS) galimybes atskleidžiant ir tiriant nusikalstamas veikas?*
- ✓ *Ar Jums yra žinoma apie DNR duomenų registro įsteigimą ir galimybes atskleidžiant ir tiriant nusikalstamas veikas?*
- ✓ *Ar ADIS ir (ar) DNR registro duomenų panaudojimas padėjo atskleisti ir tirti nusikalstamas veikas Jūsų žinioje esančiose ikiteisminio tyrimo medžiagose?*[161]

~ 94 proc. Kriminalinės policijos skyrių pareigūnai pareiškė, kad jiems yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos galimybes atskleidžiant ir tiriant nusikalstamas veikas ir apie DNR registro įsteigimą bei galimybes atskleidžiant ir tiriant nusikalstamas veikas. ~ 81 proc. šios grupės apklaustųjų tokiomis galimybėmis pasinaudojo ikiteisminio tyrimo metu, kaip priemone atskleisti nusikalstamą veiką arba jai tirti.

[160] Apskaičiuota naudojant skaičiuoklę http://www.raosoft.com/samplesize.html; prisijungimo laikas: 2013-02-28.
[161] Tik Kriminalinės policijos skyrių pareigūnams.

Apie automatizuotos daktiloskopinės identifikavimo sistemos galimybes atskleidžiant ir tiriant nusikalstamas veikas yra žinoma ir ~ 24 proc. plačiosios visuomenės nariams, o ~ 68 proc. pareiškė to nežiną. Apie DNR registro įsteigimą bei galimybes atskleidžiant ir tiriant nusikalstamas veikas, žino žymiai daugiau šios tiriamos grupės respondentų, t.y. ~ 44 proc., likusieji ~ 46 proc. pareiškė to nežiną.

3.3. Informacijos teikimas visuomenei apie biometrinių asmens tapatybės nustatymo sistemų panaudojimą ir biometrinių duomenų tvarkymą

Aiškinantis, ar visuomenės nariams yra teikiama pakankama ir išsami informacija apie biometrinių sistemų panaudojimą ir biometrinių duomenų tvarkymą, respondentams buvo užduoti klausimai:

- ✓ *Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą?*
- ✓ *Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą?*
- ✓ *Ar, Jūsų nuomone, yra pakankamai literatūros lietuvių kalba (moksliniai, mokslo populiarinimo straipsniai, knygos) apie biometrines asmens tapatybės nustatymo sistemas (toliau BATNS) ir jų panaudojimo galimybes?*[162]

~ 69 proc. Kriminalinės policijos skyrių pareigūnų pareiškė, kad jų nuomone, Lietuvoje visuomenė nėra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą, o ~25 proc. pareigūnų teigė nežiną situacijos. ~82 proc. kitos tiriamos grupės respondentų galvoja, kad tokios informacijos nėra pakankamai, ~11 proc. to nežino.

[162] Tik Kriminalinės policijos skyrių pareigūnams.

~74 proc. pareigūnų įsitikinę, kad trūksta informacijos ir apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą, ~ 13 proc. buvo manąs, kad tokios informacijos yra pakankamai ir ~ 13 proc. pasisakė nežiną. Panašiai atsakė ir plačiosios visuomenės nariai, atitinkamai ~ 79 proc. informacijos pasigenda, o ~ 16 proc. nežino ar trūksta tokios informacijos.

Be to, ~ 38 proc. pareigūnų pasigenda literatūros lietuvių kalba apie biometrinių sistemų panaudojimo galimybes, ~ 62 proc. teigė nežiną ar anksčiau minėtos literatūros trūksta.

3.4. Visuomenės suvokimas apie biometrinių asmens tapatybės nustatymo sistemų ir biometrinių duomenų panaudojimo esmę, sritis, teisinį reguliavimą

Siekiant nustatyti, ar visuomenės nariai turi bendrą supratimą apie biometrines sistemas, biometrinius duomenis, jų naudojimo esmę, sritis, teisinį reguliavimą, buvo suformuluoti šie klausimai:

- ✓ *Ar Jums yra žinoma kaip (kokiu pavidalu) yra saugomi asmens biometriniai duomenys?*
- ✓ *Ar galėtumėte nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie galėtų būti BATNS?*
- ✓ *Ar Jums yra žinoma, kokios BATNS ir kokiose srityse yra naudojamos plačiausiai užsienio šalyse?*
- ✓ *Ar, Jūsų nuomone, Europos Sąjungoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?*
- ✓ *Ar, Jūsų nuomone, Lietuvoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?*

Iš respondentų pateiktų atsakymų matyti, kad ~ 75 proc. Kriminalinės policijos skyrių pareigūnams nežinoma kaip yra saugomi asmens biometriniai duomenys, likusiems ~ 25 proc. tai yra žinoma. ~ 82 proc. plačiosios visuomenės atstovų taip pat to nežino.

Net ~81 proc. pareigūnų ir ~67 proc. plačiosios visuomenės narių negali nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie yra naudojami biometrinėse sistemose asmens tapatybei nustatyti, o ~13 proc. pareigūnų ir ~17 proc. kitos tiriamos grupės atstovų abejoja galintys tai padaryti.

~87 proc. pareigūnų ir ~70 proc. plačiosios visuomenės narių nėra žinoma kokiose srityse yra labiausiai paplitęs biometrinių sistemų panaudojimas įvairiose pasaulio šalyse, tik ~ 13 proc. pareigūnų ir ~15 proc. kitos tiriamos grupės narių tai yra žinoma.

~ 81 proc. pareigūnų teigė nežiną, ar Europos Sąjungoje yra sukurta pakankama teisinė bazė reglamentuojanti biometrinių sistemų panaudojimą teisėtvarkoje ir visuomeniniame gyvenime ir tik ~ 13 proc. tikina, kad toks reglamentavimas nėra tinkamai sureguliuotas. ~ 25 proc. plačiosios visuomenės narių mano, kad toks reglamentavimas nėra tinkamai sureguliuotas ir ~68 proc. nieko apie tai nežino.

~62 proc. pareigūnų pasisakė nežinantys, ar Lietuvoje yra sukurta pakankama teisinė bazė reglamentuojanti nagrinėjamą sritį. ~38 proc. įsitikinę, kad teisinis reguliavimas nėra pakankamas. Panašiai atsakė ir plačiosios visuomenės atstovai, ~36 proc. galvoja, kad teisinis reguliavimas nėra pakankamas ir ~68 proc. padėties nežino.

3.5. Visuomeninė nuomonė apie biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką

Siekiant atskleisti visuomenės narių nuomonę apie biometrinių sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką buvo suformuluoti klausimai:

- ✓ *Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją?*
- ✓ *Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą?*
- ✓ *Ar galėtų, Jūsų nuomone, BATNS padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas (pvz. oro uostuose, bankuose, stadionuose, masinio susibūrimo vietose, elektroninės bankininkystės sistemose kt.)?*

Atlikus duomenų analizę paaiškėjo, kad ~ 49 proc. pareigūnų galvoja, kad biometrinių sistemų panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją, ~ 38 proc. to nežino ir ~ 13 proc. įsitikinę, kad nusikalstamų veikų prevencijos tai neužtikrins. Panašiai išsidėstė ir plačiosios visuomenės atstovų apklausos rezultatai: ~ 41 proc. įsitikinę, kad galėtų,~ 45 proc. nežino ir ~ 14 proc. galvoja, kad biometrinių sistemų naudojimas negalėtų užtikrinti nusikalstamų veikų prevencijos.

~62 proc. pareigūnų ir ~48 proc. plačiosios visuomenės narių tikina, kad biometrinių sistemų panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą. ~ 38 proc. pareigūnų ir ~ 42 proc. kitos tiriamos grupės atstovų pareiškė to nežiną. Be to, ~ 10 proc. plačiosios visuomenės narių pareiškė, kad biometrinių sistemų panaudojimas Lietuvoje negali užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą.

~ 56 proc. apklaustųjų pareigūnų ir ~ 50 proc. kitos tiriamos grupės atstovų įsitikinę, kad biometrinių sistemų panaudojimas gali padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas. ~ 31 proc. pareigūnų ir ~ 40 proc. plačiosios visuomenės narių nežino ar tai įmanoma ir ~ 13 proc. pareigūnų atsakė, kad biometrinių sistemų panaudojimas negali padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas.

3.6. Tyrimo išvados

Tyrimas parodė, kad Kriminalinės policijos skyrių pareigūnai savo veikloje aktyviai naudojasi automatizuotos daktiloskopinės identifikavimo sistemos galimybėmis, DNR registro galimybėmis atskleidžiant ir tiriant nusikalstamas veikas ir jau įvertino šių priemonių efektyvumą. Plačiajai visuomenei apie tokias galimybes yra mažai žinoma. Informacijos, kiek apie automatizuotos daktiloskopinės identifikavimo sistemos egzistavimą, funkcionavimą ir galimybes, tiek apie DNR registrą yra tikrai nemažai spaudoje ir internete. Galimai ši informacija dažniausiai nėra adaptuota plačiajai visuomenei ir yra daugiau specializuota, lengviau suprantama mokslininkams, teisininkams, specialistams ir pan. Šiame magistro baigiamajame darbe tokios, pateikiamos ir prieinamos plačiajai visuomenei, informacijos turinio analizės atlikta nebuvo, tad tolimesni tyrimai galėtų tai atskleisti. Atkreiptinas dėmesys, kad nemažai plačiosios visuomenės narių pareiškė žinantys apie DNR registro galimybes, tačiau manytina, kad visuomenės nariai daugiau susidomi būtent DNR tyrimais, nes medicinos srityje (prenatalinė diagnostika, tėvystės nustatymas, genetinių ligų nustatymas ir t.t.) dabar tai itin populiaru, todėl ir jų informuotumas apie

DNR registrą, kaip parodė šis tyrimas, atrodo didesnis, negu tų pačių asmenų žinojimas apie ADIS, arba tai yra iš vis tik pseudo žinojimas.

Informacijos apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą, apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą, literatūros lietuvių kalba apie biometrinių sistemų panaudojimo galimybes yra nedaug, esama informacija galimai sunkiai suvokiama eiliniam vartotojui, nes pateikiama neadaptuota plačiajai visuomenei. Pateikiamos informacijos turinį, ir turinio kaitos tendencijas galėtų atskleisti tolimesni tyrimai.

Plačiosios visuomenės supratimas apie biometrines sistemas, biometrinius duomenis, jų naudojimo esmę, sritis, teisinį reguliavimą taip pat menkas. Mokslinių populiarinimo straipsnių, kitos informacijos tiriama tematika nėra daug, tačiau kai kurie tiriamų problemų aspektai yra pateikiami ir plačiajai visuomenei. Tokios informacijos pateikimas yra tikslingas skaitomiausiose internetinėse svetainėse, elektroniniuose žurnaluose, spaudoje ir kituose šaltiniuose. Taip, pvz., VDAI 2013 m. pradžioje, atnaujinus savo interneto svetainę, žymiai daugiau dėmesio skiria visuomenės informavimui ir viešosioms konsultacijoms.

Prielaida, kad Kriminalinės policijos skyrių pareigūnai turi daugiau žinių apie biometrinių sistemų naudojimo ypatumus, tikslus, galimybes, o kitos tiriamos grupės atstovai tokių žinių turi mažiau arba visai neturi nepasitvirtino, o kai kuriais atvejais rezultatas yra net priešingas. Darytina išvada, kad pareigūnai žino tik tiek kiek jiems priklauso dėl jų tarnybinės veiklos, o kita informacija jiems galimai yra nenaudinga, nebūtina, neįdomi arba dėl kitų priežasčių – šie klausimai liko neišsiaiškinti. Atlikus tokių priežasčių tyrimą, esant poreikiui, galima spręsti klausimą dėl mokymo programos sudarymo, kvalifikacijos tobulinimo kursų tikslinėse grupėse organizavimo.

Pažymėtina, kad pusė apklaustųjų respondentų mano, kad biometrinių sistemų panaudojimas galėtų ne tik užtikrinti nusikalstamų veikų atskleidimą ir tyrimą, bet ir jų prevenciją. Taip pat šių sistemų panaudojimas gali padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas.

Apibendrinus tyrimo rezultatus galima padaryti šias išvadas:

1. Visuomenės informuotumas apie esamų Lietuvoje biometrinių sistemų praktinio panaudojimo privalumus teisėsaugos srityje yra mažas, jei tai nesusieta su tarnybine veikla;
2. Visuomenei nėra teikiama pakankama ir išsami informacija apie biometrinių sistemų panaudojimą ir biometrinių duomenų tvarkymą;

3. Bendras visuomenės narių supratimo lygis apie biometrines sistemas, biometrinius duomenis, jų naudojimo esmę, sritis, teisinį reguliavimą yra žemas;
4. Visuomenė tiki, kad biometrinių sistemų panaudojimas galėtų užtikrinti nusikalstamų veikų atskleidimą ir tyrimą, nusikalstamų veikų prevenciją, gali padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas;
5. Kriminalinės policijos skyrių pareigūnai savo veikloje aktyviai naudojasi automatizuotos daktiloskopinės identifikavimo sistemos galimybėmis, DNR registro galimybėmis atskleidžiant ir tiriant nusikalstamas veikas, tačiau daugiau žinių apie biometrinių sistemų panaudojimo galimybes kitose srityse neturi. Taip pat jiems nėra žinoma ar ES ir Lietuvos Respublikoje yra sukurta pakankama teisinė bazė reglamentuojanti biometrinių sistemų panaudojimą ir asmens biometrinių duomenų tvarkymą, o taip pat pasigenda informacijos, specialiosios literatūros apie biometrinių sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką.

IŠVADOS IR PASIŪLYMAI

Išnagrinėjus biometrinių asmens tapatybės nustatymo sistemų veikimo principus ir šių sistemų panaudojimo aspektus įvairiose šalyse ir Lietuvos Respublikoje užtikrinant visuomenės saugumą ir viešąją tvarką buvo nustatyta:

1. Šiuolaikinės biometrinės sistemos leidžia greitai ir tiksliai išskirti ir atpažinti asmenį iš kitų pagal tam tikrus unikalius jo *fizinius, fiziologinius požymius* arba *elgesio savybes*, o tam tikros biometrinės sistemos pasirinkimas priklauso visų pirma nuo dviejų parametrų: *saugumo* ir būtent šios biometrinės sistemos naudojimo *tikslingumo.* Per pastaruosius 12 metų aktyvus biometrinių sistemų panaudojimas įvairiais tikslais viešajame ir privačiame sektoriuje smarkiai užaugo, o pamatinis šių sistemų panaudojimo tikslas yra visų pirma siekis užtikrinti visuomenės saugumą ir viešąją tvarką.
2. Populiariausi asmens atpažinimo metodai naudojami biometrinėse sistemose yra atpažinimas pagal *pirštų papiliarinį raštą* ir atpažinimas pagal *unikalius veido požymius.* Dideles perspektyvas turi asmens atpažinimo pagal *akies rainelės piešinį* metodas, nes tokios sistemos dabar atpigo, yra labai patikimos ir leidžia atpažinti per atstumą net judantį žmogų. Kompleksinis asmens atpažinimo metodų naudojimas daugiarūšėse biometrinėse sistemose didina efektyvumą, tikslumą ir padeda išvengti klaidų.
3. Biometrinių sistemų panaudojimas Lietuvos Respublikoje priklauso nuo valstybės teisinių prievolių, vykdant tarptautinių ir ES sutarčių įsipareigojimus, o tai pat valstybės ir visuomenės interesų bei poreikių, kuriuos veikia išoriniai veiksniai, tokie kaip ES reikalavimai, kitų valstybių patirtis. Lietuvos Respublikoje biometrinės sistemos yra naudojamos teisėsaugos srityje, pasienio kontrolės punktuose, o taip pat viešajame sektoriuje – bankuose, valstybės įmonėse, įstaigose, organizacijose praėjimo kontrolės tikslais, kompiuterinės informacijos apsaugai užtikrinti. Privačiame sektoriuje biometrinės sistemos naudojamos labai retai.

Išnagrinėjus biometrinių asmens tapatybės nustatymo sistemų praktinio realizavimo galimybes ir pagrindinius asmens biometrinių duomenų tvarkymo teisinio reguliavimo aspektus ES ir Lietuvos Respublikoje buvo nustatyta:

1. Dėl spartaus biometrinių technologijų vystymosi atsiranda asmens biometrinių duomenų apsaugos taisyklių trūkumų ir šių taisyklių modernizavimo būtinumo problemos, nes platus ir nekontroliuojamas asmens biometrinių duomenų naudojimas kelia susirūpinimą

dėl žmonių pagrindinių *teisių* ir *laisvių apsaugos*. Valstybėse ES narėse galiojančios taisyklės dėl asmens biometrinių duomenų tvarkymo labai skiriasi, o duomenų valdytojai laikosi skirtingų nacionalinės teisės aktų ir reikalavimų.

2. ES svarbiausias galiojantis asmens biometrinių duomenų tvarkymą reglamentuojantis teisės aktas yra Direktyva 95/46/EB, pagal kurią, *proporcingumo* principo laikymasis yra asmens biometrinių duomenų tvarkymo šerdis, taip pat būtinas *teisėtumo ir būtinumo* įvertinimas, atsižvelgiant į riziką asmens pagrindinių teisių ir laisvių apsaugai.
3. Direktyva 95/46/EB yra įgyvendinta Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (ADTAĮ), kuris reglamentuoja, kad biometriniai asmens duomenys turi būti tvarkomi tik jeigu tam yra *teisinis pagrindas*, duomenų tvarkymas yra *tinkamas*, *svarbus* ir *neperteklinis* atsižvelgiant į *tikslus*, kuriais duomenys renkami, o naudojant biometrines sistemas, turi būti įvertintas visų pirma tvarkomų asmens biometrinių duomenų *proporcingumas* ir *būtinumas*. Kadangi sąvokos *asmens biometriniai duomenys* ADTAĮ nėra išskirta ir nėra aiškaus vaizdo, kada asmens biometriniai duomenys bus laikomi ypatingais asmens duomenimis, o kada tokiais nebus laikomi – duomenų valdytojui, duomenų tvarkytojui ir duomenų subjektui gali kilti neaiškumų ir klausimų, kaip taikyti ADTAĮ vienu ir kitu atveju.
4. Lietuvos Respublikoje galiojantys teisės aktai, susiję su biometrinių duomenų tvarkymu ir apsauga, iš esmės atitinka ES teisės aktuose keliamus reikalavimus, tačiau esami įstatymai Lietuvoje, reglamentuojantys asmens duomenų tvarkymą, nebuvo patikrinti biometrinių duomenų kontekste. Pagrindinės rizikos, galinčios atsirasti naudojant biometrines sistemas, yra asmens biometrinių duomenų neteisėtas naudojimas, biometrinių sistemų veikimo sutrikimai, galimas piktnaudžiavimas biometriniais duomenimis.

Atlikus visuomenės požiūrio į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje tyrimą, gauti rezultatai parodė:

1. Visuomenei nėra teikiama pakankama ir išsami informacija apie biometrinių sistemų panaudojimą ir asmens biometrinių duomenų tvarkymą, todėl visuomenės narių bendro supratimo lygis apie biometrines sistemas, asmens biometrinius duomenis, jų panaudojimo esmę, sritis, teisinį reguliavimą yra žemas, tačiau visuomenė tiki, kad biometrinių sistemų panaudojimas galėtų užtikrinti nusikalstamų veikų atskleidimą ir

tyrimą, nusikalstamų veikų prevenciją, gali padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas.

2. Kriminalinės policijos skyrių pareigūnai savo veikloje aktyviai naudojasi automatizuotos daktiloskopinės identifikavimo sistemos galimybėmis, DNR registro galimybėmis atskleidžiant ir tiriant nusikalstamas veikas, tačiau daugiau žinių apie biometrinių sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką kitose srityse neturi.
3. Kriminalinės policijos skyrių pareigūnams nėra žinoma ar ES ir Lietuvos Respublikoje yra sukurta pakankama teisinė bazė reglamentuojanti biometrinių sistemų panaudojimą ir asmens biometrinių duomenų tvarkymą bei pasigenda informacijos ir specialiosios literatūros apie biometrinių sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką.

Atsižvelgiant į atlikto darbo rezultatus, naudojant biometrines asmens tapatybės nustatymo sistemas bei tvarkant asmens biometrinius duomenis Lietuvos Respublikoje, yra siūloma:

1. Siekiant duomenų subjektui geriau kontroliuoti savo asmens biometrinių duomenų tvarkymą, teikti pirmenybę tokių biometrinių metodų taikymui biometrinėse sistemose, kurie užtikrintų *proporcingumo* principo laikymąsi, kai biometriniai duomenys nėra gaunami iš asmenims nežinant paliktų fizinių pėdsakų, ar kai biometriniai duomenys saugomi decentralizuotai.
2. Siekiant išvengti biometrinių duomenų panaudojimo kitais, nei numatytais teisės aktais tikslais, biometriniai asmens duomenys, kada tai tik įmanoma, turėtų būti saugomi tik kaip biometrinis šablonas (modelis), iš kurio pirminio biometrinių duomenų vaizdo atkurti nebūtų galima.
3. Siekiant užkirsti kelią biometrinės informacijos saugojimui ilgiau, nei būtina tais tikslais, kuriais ji buvo surinkta arba vėliau tvarkoma, siekiant apsaugoti informaciją nuo neteisėto šių duomenų gavimo, turi būti parengti tinkami automatinio duomenų ištrynimo teisiniai pagrindai ir numatyti atitinkami techniniai sprendimai.
4. Siekiant, kad biometrinių duomenų subjektai suprastų ir galėtų naudotis savo teisėmis tvarkant jų biometrinius duomenis, bet kokia informacija duomenų subjektui turėtų būti lengvai prieinama, paprastai ir aiškiai suformuluota.
5. Siekiant prevenciniais veiksmais užtikrinti veiksmingą duomenų subjektų teisių ir laisvių apsaugą, VDAĮ turi teikti daugiau viešųjų konsultacijų visuomenei bei paruošti rekomendacijas duomenų valdytojams, duomenų tvarkytojams apie biometrinių sistemų

praktinį naudojimą ir biometrinių duomenų tvarkymą, inicijuoti informacijos teikimą duomenų valdytojams ir duomenų tvarkytojams nuo pačios pradžios, t.y. nuo sumanymo diegti biometrinę sistemą.

6. Siekiant tobulinti nusikalstamų veikų prevencijos bei kontrolės sistemą, VRM turėtų inicijuoti galimybių, sujungiant asmens atpažinimo pagal veidą biometrines sistemas su esamomis vaizdo stebėjimo sistemomis, tyrimą, o taip pat, išnagrinėjus galimybes ir poreikį, pavesti Policijos departamentui aktyviai teikti informaciją visuomenei apie biometrinių sistemų panaudojimo galimybes viešajame ir privačiame sektoriuje užtikrinant visuomenės saugumą ir viešąją tvarką.

Magistro baigiamasis darbas baigtas: 2013 04 24

Magistrantė Olga Trukšina

oltruksina@stud.mruni.eu

LITERATŪROS SĄRAŠAS

Lietuvos Respublikos teisės aktai:

1. Lietuvos Respublikos Konstitucija // Valstybės žinios. 1992, Nr. 33-1014.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.
3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas // Valstybės žinios. 2008, Nr. 22-804.
4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 1, 2, 3, 6, 20, 21, 22, 24, 25, 26, 27, 29, 33, 35, 36, 38, 40, 45, 53 straipsnių, ketvirtojo ir devintojo skirsnių pavadinimų pakeitimo ir papildymo ir įstatymo papildymo 13^1, 15^1, 35^1, 41^1 straipsniais įstatymas // Valstybės žinios. 2011, Nr. 65-3046.
5. Lietuvos Respublikos asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas // Valstybės žinios. 2011, Nr. 52-2511.
6. Lietuvos Respublikos asmens tapatybės kortelės įstatymas // Valstybės žinios. 2001, Nr. 97-3417.
7. Lietuvos Respublikos asmens tapatybės kortelės įstatymo 2, 4, 5 straipsnių pakeitimo bei papildymo ir įstatymo papildymo 1^1 straipsniu įstatymas // Valstybės žinios. 2008, Nr. 76-3007.
8. Lietuvos Respublikos asmens tapatybės kortelės įstatymo 2, 5, 6, 7 straipsnių pakeitimo ir papildymo įstatymas // Valstybės žinios. 2010, Nr. 125-6379.
9. Lietuvos Respublikos baudžiamojo proceso kodeksas // Valstybės žinios. 2002, Nr. 37-1341.
10. Lietuvos Respublikos „dėl užsieniečių teisinės padėties" įstatymas // Valstybės žinios. 2004, Nr. 73-2539.
11. Lietuvos Respublikos įstatymo „dėl užsieniečių teisinės padėties" 1, 2, 6, 9, 10, 11, 12^1, 17, 19, 21, 22, 24, 26, 33, 37, 38, 40, 43, 49^1, 50, 53, 54, 55, 57, 58, 89, 97, 98, 99, 100, 101, 102, 104, 106, 113, 128, 131, 133, 139, 140^1, 141^1 straipsnių ir priedo pakeitimo ir papildymo, įstatymo papildymo 44^1, 49^3, 98^1, 99^1, 103^1, 105, 105^1, 105^2, 105^3, 105^4, 106^1 straipsniais ir 12^2, 13, 14, 15, 16, 18, 20, 145 straipsnių pripažinimo netekusiais galios įstatymas // Valstybės žinios. 2012, Nr. 85-4450.

12. Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2000, Nr. 61-1827.
13. Lietuvos Respublikos gyventojų registro įstatymas // Valstybės žinios. 1992, Nr. 5-78.
14. Lietuvos Respublikos gyventojų registro įstatymo 4, 9, 11 straipsnių pakeitimo ir papildymo įstatymas // Valstybės žinios. 2006, Nr. 65-2387.
15. Lietuvos Respublikos gyventojų registro įstatymo 7, 9, 11 straipsnių pakeitimo ir papildymo įstatymas // Valstybės žinios. 2012, Nr. 80-4142.
16. Lietuvos Respublikos kriminalinės žvalgybos įstatymas // Valstybės žinios. 2012, Nr. 122-6093.
17. Lietuvos Respublikos paso įstatymas // Valstybės žinios. 2001, Nr. 99-3524.
18. Lietuvos Respublikos paso įstatymo 1, 4 straipsnių pakeitimo ir papildymo bei įstatymo papildymo priedu įstatymas // Valstybės žinios. 2006, Nr. 77-2957.
19. Lietuvos Respublikos policijos veiklos įstatymas // Valstybės žinios. 2000, Nr. 90-2777.
20. Lietuvos Respublikos policijos veiklos įstatymo 1, 2, 3, 6^2, 7, 11, 12, 15, 16, 18, 19 straipsnių pakeitimo ir papildymo įstatymas // Valstybės žinios. 2009, Nr. 130-5637.
21. Lietuvos Respublikos tarnybinio paso įstatymas // Valstybės žinios. 2000, Nr. 7-178.
22. Lietuvos Respublikos tarnybinio paso įstatymo 1, 5 straipsnių pakeitimo ir papildymo bei įstatymo papildymo priedu įstatymas // Valstybės žinios. 2006, Nr. 77-2958.
23. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu // Valstybės žinios. 2001, Nr. 32-1059.
24. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija // Valstybės žinios. 2000, Nr. 96-3016.
25. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) ir Europos Tarybos Ministrų Komiteto 2001 m. lapkričio 8 d. Konvencijos ETS Nr. 108 papildomas protokolas dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų // Valstybės žinios. 2001, Nr. 32-1059.
26. Konvencija dėl informacijos technologijų naudojimo muitinės tikslais, parengta vadovaujantis Europos Sąjungos sutarties K.3 straipsniu // Valstybės žinios. 2004, Nr. 112-4179.
27. Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo // Valstybės žinios. 2001, Nr. 32-1055.
28. Lietuvos Respublikos įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu papildomo protokolo dėl priežiūros institucijų ir valstybės sienas kertančių duomenų srautų ratifikavimo // Valstybės žinios. 2004, Nr. 36-1177.

29. Lietuvos Respublikos įstatymas dėl Konvencijos dėl informacijos technologijų naudojimo muitinės tikslais, parengtos vadovaujantis Europos Sąjungos sutarties K.3 straipsniu, jos protokolų ir susitarimo dėl laikino Konvencijos taikymo ratifikavimo // Valstybės žinios. 2004, Nr. 67-2356.
30. Visuotinė žmogaus teisių deklaracija // Valstybės žinios. 2006, Nr. 68-2497.
31. Lietuvos Respublikos Vyriausybės 2004 m. gruodžio 6 d. nutarimas Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą" // Valstybės žinios. 2004, Nr. 177-6569.
32. Lietuvos Respublikos Vyriausybės 2009 m. balandžio 15 d. nutarimas Nr. 310 „Dėl tarybos sprendimo 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje, įgyvendinimo veiksmų plano patvirtinimo" // Valstybės žinios. 2009, Nr. 49-1957.
33. Lietuvos Respublikos Vyriausybės 2009 m. gruodžio 23 d. nutarimas Nr. 1706 „Dėl 2009 m. balandžio 6 d. Tarybos sprendimo 2009/371/TVR dėl Europos policijos biuro (Europolo) įsteigimo įgyvendinimo" // Valstybės žinios. 2009, Nr. 153-6933.
34. Lietuvos Respublikos Vyriausybės 2009 m. lapkričio 4 d. nutarimas Nr. 1456 „Dėl Lietuvos nacionalinės vizų informacinės sistemos įsteigimo, jos nuostatų patvirtinimo ir veiklos pradžios nustatymo" // Valstybės žinios. 2009, Nr. 136-5933.
35. Lietuvos Respublikos Vyriausybės 2009 m. rugsėjo 30 d. nutarimas Nr. 1244 „Dėl Lietuvos Respublikos Vyriausybės teisėkūros taisyklių patvirtinimo" // Valstybės žinios. 2009, Nr. 121-5212.
36. Lietuvos Respublikos Vyriausybės 2011 m. lapkričio 9 d. nutarimas Nr. 1324 „ Dėl tarpvalstybinio keitimosi DNR duomenimis, daktiloskopiniais duomenimis, transporto priemonių registracijos, jų savininkų ir valdytojų duomenimis ir informacija, susijusia su didelio masto tarpvalstybinio pobūdžio renginiais ar teroristinių nusikaltimų prevencija, tvarkos aprašo patvirtinimo" // Valstybės žinios. 2011, Nr. 137-6494.
37. Lietuvos Respublikos Vyriausybės 2011 m. gegužės 4 d. nutarimas Nr. 522 „Dėl 2009 m. lapkričio 30 d. Tarybos sprendimo 2009/917/TVR dėl informacinių technologijų naudojimo muitinės tikslais įgyvendinimo" // Valstybės žinios. 2011, Nr. 55-2645.
38. Lietuvos policijos generalinio komisaro įsakymas Nr. 5-V- 42 „Dėl DNR duomenų registro steigimo ir nuostatų patvirtinimo" // Valstybės žinios. 2011, Nr.10-475.

39. Lietuvos policijos generalinio komisaro įsakymas Nr. 5-V-41 dėl Lietuvos policijos generalinio komisaro 2007 m. vasario 5 d. įsakymo Nr. 5-V-88 „Dėl Lietuvos policijos daktiloskopinių duomenų registro steigimo" pakeitimo // Valstybės žinios. 2011, Nr. 137-6494.
40. Lietuvos policijos generalinio komisaro įsakymas Nr. 5-V-88 „Dėl Lietuvos policijos daktiloskopinių duomenų registro steigimo" // Valstybės žinios. 2007, Nr. 19-751.
41. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2006 m. vasario 2 d. įsakymas Nr. 1T-6 „Dėl išankstinės patikros atlikimo taisyklių patvirtinimo" // Valstybės žinios. 2006, Nr. 18-653; 2009, Nr. 11-447; 2011, Nr. 104-4899.
42. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymas Nr. 1T-71(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo" // Valstybės žinios. 2008, Nr. 135-5298.
43. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. spalio 27 d. įsakymas Nr. 1T-64(1.12) „Dėl duomenų valdytojų atsakymo Valstybinei duomenų apsaugos inspekcijai dėl duomenų subjekto teisės susipažinti su savo asmens duomenimis įgyvendinimo pateikimo tvarkos aprašo patvirtinimo" // Valstybės žinios. 2008, Nr. 125-4790.
44. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2009 m. sausio 16 d. įsakymas Nr. 1T-5(1.12) „Dėl Duomenų apsaugos priemonių aprašo formos patvirtinimo" // Valstybės žinios. 2009, Nr. 11-448.
45. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2010 m. gruodžio 30 d. įsakymas Nr. 1T-104(1.12) „Dėl Valstybinės duomenų apsaugos inspekcijos vykdomų patikrinimų atlikimo taisyklių patvirtinimo" // Valstybės žinios. 2011, Nr. 1-24.

Tarptautiniai ir Europos Sąjungos teisės aktai:

46. 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 // OL 2004 m. specialusis leidimas, 13 skyrius. T.15. P. 355.
47. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) // OL 2004 m. specialusis leidimas, 13 skyrius. T.29. P.514 su paskutiniais pakeitimais 2009/136/EB // OL 2009 L337. P. 11.

48. 2006 m. gruodžio 20 d. Europos Parlamento ir Tarybos reglamentas 1987/2006/EB dėl antrosios kartos Šengeno informacinės sistemos sukūrimo, veikimo ir naudojimo (SISII) // OL 2006 L 381/4.
49. 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos // OL 2008 L 350. P. 60.
50. 2009 m. gegužės 28 d. Europos Parlamento ir Tarybos reglamentas 444/2009/EB iš dalies keičiantis Tarybos reglamentą 2252/2004/EB dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų // OL 2009 L 142/1.
51. 2009 m. lapkričio 30 d. Tarybos sprendimas 2009/917/TVR dėl informacinių technologijų naudojimo muitinės tikslais // OL 2009 L 323. P. 20.
52. 2010 m. vasario 5 d. Komisijos sprendimas 2010/87/ES dėl sutarčių standartinių sąlygų, nustatytų asmens duomenų perdavimui trečiosiose šalyse įsikūrusiems tvarkytojams pagal Europos Parlamento ir Tarybos direktyvos 95/46/EB nuostatas // OL 2010 L 39. P. 5.
53. Europos Sąjungos pagrindinių teisių chartija // OL 2007 C 303/01.
54. Konvencija dėl Šengeno susitarimo, 1985 m. birželio 14 d. sudaryto tarp Beniliukso ekonominės sąjungos valstybių, Vokietijos Respublikos ir Prancūzijos Respublikos vyriausybių dėl laipsniško jų bendrų sienų kontrolės panaikinimo, įgyvendinimo // OL 2004 m. specialusis leidimas, 19 skyrius. T.2. P.9 su paskutiniais pakeitimais, padarytais 2005 m. liepos 6 d. Europos Parlamento ir Tarybos reglamentu (EB) Nr. 1160/2005 // OL 2005 L 191. P. 18.
55. Lisabonos sutartis // OL 2007 C 306.
56. Sutartis dėl Europos Sąjungos veikimo // OL 2012 C 326.

Knygos, publikacijos:

57. Ivanovas E. Biometriniai požymiai asmens atpažinimo sistemose // Mokslas Lietuvos ateitis, 2010. T.2, Nr.1. P. 23-26.
58. Kardelis K. Mokslinių tyrimų metodologija ir metodai. – Kaunas: Judex, 2002.
59. Kvietkauskas V. ir kt. Tarptautinių žodžių žodynas. – Vilnius: K. Poželos spaustuvė, 1985. P. 527.
60. Novikovas A. Viešosios tvarkos, kaip viešojo saugumo sudedamosios dalies, turinio analizė // Verslo ir teisės aktualijos. – Vilnius: Vilniaus teisės ir verslo kolegija, 2008. T.2. P. 85-93.
61. Stupak V., Vasiliauskas R. Autentifikavimo procedūrų nagrinėjimo informatikos ir informacinių

technologijų studijose aspektai // Teoriniai ir praktiniai statutinių pareigūnų rengimo aspektai: Respublikinės mokslinės konferencijos straipsnių rinkinys. – Kaunas: Mykolo Romerio universitetas, 2005. P. 101-110.

62. Stupak V., Vasiliauskas R. Biometrinių atpažinimo sistemų efektyvumo nagrinėjimo informatikos studijose aspektai // Policijos pareigūnų profesinio rengimo aktualijos. Mokslinių straipsnių rinkinys. – Kaunas: Mykolo Romerio universiteto Viešojo saugumo fakultetas, 2007. P. 87-95.
63. Stupak V., Vasiliauskas R. Biometrinių autentifikavimo sistemų nagrinėjimo informatikos studijose aspektai // Policijos pareigūnų profesinio rengimo aktualijos. Mokslinių straipsnių rinkinys. – Kaunas: Mykolo Romerio universiteto Viešojo saugumo fakultetas, 2007. P. 79-86.
64. Šlapkauskas V. Visuomenės saugumo ir žmogaus teisių ryšys kaip antiterorizmo ideologijos legitimacijos pagrindas // Jurisprudencija: mokslo darbai. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2005. T.68(60). P. 25-34.
65. Torvaldas J. Kriminalistikos keliai ir klystkeliai. – Vilnius: Mintis, 1981. P. 383.
66. Venčkauskas A., Toldinas J. Kompiuterių ir operacinių sistemų sauga: mokomoji knyga. – Kaunas: Kauno technologijos universitetas, 2008. P. 200.

Šaltiniai iš interneto svetainių lietuvių kalba:

67. Asmens duomenų apsaugos naujienų biuletenis. 2012 m. sausis-vasaris Nr.1(46) // http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/BiulNr1_2012.pdf; prisijungimo laikas: 2012-10-24.
68. Biometrinių duomenų naudojimo apraiškos Europoje. 2008 // http://www.ada.lt/images/cms/File/Biometriniai%20duomenys%20(Galutinis)%2020080618.doc; prisijungimo laikas: 2012-10-19.
69. Biometriniu duomenų patikra pasienyje jau veikia. 2012 // http://atea.lt/news/biometriniu-duomenu-patikra-pasienyje-jau-veikia/ ; prisijungimo laikas: 2012-11-08.
70. Būtina išsami diskusija apie planuojamą biometrinių duomenų naudojimą. Viešas pareiškimas 2006//http://www.hrmi.lt/uploaded/PDF%20dokai/Biometriniu%20duomenu%20naudojimas_viesas%20pareiskimas_2006.pdf; prisijungimo laikas: 2012-10-19.

71. Darbinis dokumentas dėl biometrinių duomenų 12168/02/EN WP 80. 29 straipsnio – duomenų apsaugos darbo grupė. 2003 m. rugpjūčio 1d. //http://www.ada.lt/images/cms/File/WP80.pdf ; prisijungimo laikas: 2011-11-20.
72. Gricukas G. Biometrija: iš naujo apie naudą ir patikimumą. 2008 //http://www.technologijos.lt/n/technologijos/technologiju_rinka/straipsnis?name=straipsnis-5833; prisijungimo laikas: 2011-11-20.
73. Išorės sienų fondo 2010 m. metinė programa//http://www.vrm.lt/fileadmin/Padaliniu_failai/ES_paramos_administravimo/ISf/ISF-2010_LT_RUGSEJO_15.doc; prisijungimo laikas: 2012-11-08.
74. Jonaitis A. Akys nemeluoja, pirštai garantuoja. 2007 //http://www.elektronika.lt/straipsniai/pazintiniai/9714/akys-nemeluoja-pirstai-garantuoja; prisijungimo laikas: 2011-11-17.
75. Komisijos komunikatas Europos Parlamentui ir Tarybai ,,Laisvės, saugumo ir teisingumo erdvė piliečių labui", COM(2009) 262 //http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=lt&DosId=198336; prisijungimo laikas: 2012-10-25.
76. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui ,,Visapusiškas požiūris į asmens duomenų apsaugą Europos.Sąjungoje".COM(2010)609//http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:LT:HTML; prisijungimo laikas: 2012-11-11.
77. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui ,,Sukurti laisvės, saugumo ir teisingumo erdvę Europos.piliečiams",.COM(2010)171//http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:LT:PDF; prisijungimo laikas: 2012-10-25.
78. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui ,,Privatumo apsauga glaudžiai susijusiame pasaulyje, Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje", COM(2012) 09 // EUR-Lex-2012DC0009LT.http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT; prisijungimo laikas: 2012-10-25.
79. Kranauskas E. Asmens identifikavimas pagal veidą ir akies rainele. Daktaro disertacijos santrauka. Fiziniai mokslai, informatika (09 p). Vilniaus Universitetas. Vilnius, 2010 // http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2010~D_20100213_102112-81518/DS.005.0.01.ETD; prisijungimo laikas: 2013-01-30.

80. Lietuvos mokslininkai išrado judančio žmogaus tapatybės identifikavimo įrenginį. 2013 // http://www.veidas.lt/lietuvos-mokslininkai-israd o-judancio-zmogaus-tapatybes identifikavimo-irengini; prisijungimo laikas: 2013-02-20.
81. Lietuvos policija atnaujina technologijas. 2003 //http://www.penki.lt/LT/article.im?id=97093&tid=41; prisijungimo laikas: 2011-10-21.
82. Lietuvos policijos Kriminalistinių tyrimų centro 2009-2011m. veiklos atskaitos // http://ktc.policija.lt/lt/veikla/planai_ir_ataskaitos.html; prisijungimo laikas: 2011-10-21.
83. Lietuvos Respublikos pasas // http://www.dokumentai.lt/viewpage.php?page_id=54; prisijungimo laikas: 2011-11-29.
84. Nauja ADIS padės atskleisti dvigubai daugiau nusikaltimų // Pasienio kelias Nr.5. 1(2) // http://www.vrm.lt/fileadmin/Padaliniu_failai/Rysiu_su_visuomene_sk/visokie/pasiulymai/Pasienis_Nr.2.pdf ; prisijungimo laikas: 2011-11-20.
85. LPKTC 2012 m. veiklos ataskaita, 2012 //http://ktc.policija.lt/lt/veikla/planai_ir_ataskaitos.html; prisijungimo laikas: 2013-12-19.
86. Nuomonė 3/2005 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 //http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_lt.pdf; prisijungimo laikas: 2013-02-16.
87. Nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių 00720/12/LT WP 193. 29 straipsnio.darbo grupė. 2012 m. balandžio 27 d. //http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm; prisijungimo laikas: 2012-12-20.
88. Pasirašyta peticija į Europos Tarybą dėl biometrinių duomenų naudojimo. 2011 // http://www.hrmi.lt/./naujiena/600/; prisijungimo laikas: 2012-12-14.
89. Pasiūlymas Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo. COM(2012) 010. Aiškinamasis memorandumas 2012 // http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:LT:HTML; prisijungimo laikas: 2013-02-16.

90. Mikulskienė B. „Viešasis sektorius XXI amžiuje". Pranešimas Valstybės kontrolės konferencija „Koks turi būti viešasis sektorius?", 2011 // http://www.vkontrole.lt/page.aspx?id=15; prisijungimo laikas: 2012-11-03.
91. Viešoji konsultacija dėl pirštų atspaudų ir pagal juos sukurtų modelių tvarkymo // http://www.ada.lt/images/cms/File/viesos%20konsultacijos/pirstu_anspaud.pdf; prisijungimo laikas: 2013-02-18.
92. Žmogaus kūnas tapo unikaliu slaptažodžiu. 2008 //http://www.penki.lt/LT/article.im?id=184018&tid=41; prisijungimo laikas: 2012-02-12.
93. Žmogaus teisių stebėjimo instituto 2011 m. veiklos ataskaita. Vilnius, 2012 // http://www.hrmi.lt/uploaded/PDF%20dokai/Ataskaita__ZTSI_GALUTINE_2011_1.pdf; prisijungimo laikas: 2012-10-24.

Šaltiniai anglų kalba:

94. Amid Privacy Fears, Police Across the Nation Will Roll Out Face-Recognizing iPhone Tech This Year. 2011 // http://www.popsci.com/technology/article/2011-07/amid-privacy-fears-police-across-nation-will-roll-out-face-recognizing-iphone-tech-year; prisijungimo laikas: 2012-11-05.
95. Cavoukian A., Stoianov A., Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy. 2007 // http://www.ipc.on.ca/images/resources/bio-encryp.pdf; prisijungimo laikas: 2012-10-17.
96. Darma Putra I., Sentosa M. A. Hand Geometry Verification based on Chain Code and Dynamic Time Warping // International Journal of Computer Applications (0975 – 8887). Vol. 38–No.12, 2012. P. 17.
97. Daugman J.G. How Iris Recognition Works // IEEE Transactions on Circuits and Systems for Video Technology, 2004. Vol.14, P. 21-30.
98. EU 'Smart Borders': Commission wants easier access and enhanced security. European Commission - Press release. 2011 // http://europa.eu/rapid/press-release_IP-11-1234_en.htm; prisijungimo laikas: 2012-12-18.
99. Jain A. K. and Feng J. Latent Fingerprint Matching. MSU Technical Report, MSU-CSE-09. 2009 // http://www.cse.msu.edu/~rossarun/pubs/FengJainRoss_AlteredFingerprint_TechReport09.pdf; prisijungimo laikas: 2013-02-12.
100. Jain A. K. Biometrics: Personal Identification in Networked Society // Kluwer Academic Publishers, 1999. P. 347.

101. Makarski R. A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security, 2002. P. 46. // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407611; prisijungimo laikas: 2012-10- 03.

102. McLaren S. Reliability of iris recognition as a means of identity verification and future impact on transportation worker identification credential. Monterey, California, 2008. P. 11-16. // http://cisr.nps.edu/downloads/theses/08thesis_mclaren.pdf; prisijungimo laikas: 2012-11-15.

103. Trauring M. Automatic comparison of finger ridge patterns // Hughes Research Laboratories, Report Nr.190. Rev. April, 1963.

104. Park U., Tong Y. and Jain A. K. Face Recognition with Temporal Invariance: A 3D Aging Model. 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition, Amsterdam, Netherlands, September 2008 / /http://biometrics.cse.msu.edu/Publications/Face/ParkTongJainTemporalFaceRec_2008.pdf.; prisijungimo laikas: 2011-11-12.

105. Police mobile fingerprinting trial expands. 2008 // http://www.npia.police.uk/en/10652.htm.; prisijungimo laikas: 2012-11-05.

106. Privacy and Data Security Targets of Mytec's Commercialization Strategy // PR Newswire, 1997. P. 24.

107. Spinella E. Biometric Scanning Technologies: Finger, Facial and Retinal Scanning. SANS GSEC, San Francisco, 2003. P. 8-10.

108. Sprokkereef A., De Hert P. Ethical practice in the use of biometric identifiers within the EU // Law, Science and Policy, 2007. Vol. 3. P. 181–201.

109. Stan Z. Li, Jain A.K. Enciplopedia of biometrics. – Springer, 2009.

110. Stringer D. Arrests underline security jitters before Games. 2012 // http://www.nbcolympics.com/news-blogs/2012/arrests-underline-security-jitters-before-olympics.html; prisijungimo laikas: 2012-11-01.

111. Umut Uludag, Secure Biometric Systems. Ph.D. Thesis, 2006 / /http://biometrics.cse.msu.edu/Publications/Thesis/UmutUludag_SecureBiometrics_PhD06.pdf; prisijungimo laikas: 2012-11-02.

Kiti interneto svetainių adresai:

112. http://archyvas.infobalt.lt/main.php?&i=1123;
113. http://www.acuity-mi.com/FOB_Report.php;
114. http://www.biolink.ru/technology/biometric.php;
115. http://www.biometrics.ru;
116. http://www.dhs.gov/us-visit-office;
117. http://www.dokumentai.lt/viewpage.php?page_id=49#atk 2009;
118. http://findbiometrics.com/companies/;
119. http://www.fima.lt/#sprendimai;
120. http://www.frost.com/prod/servlet/research.pag.;
121. http://www.fujitsu.com/us/services/biometrics/palm-vein/;
122. http://www.godlikeproductions.com/forum1/message1702000/pg1;
123. http://www.ivpk.lt;
124. http://www.raosoft.com/samplesize.html;
125. http://www.veidas.lt/lietuviskos-imones-uzsienyje-isgarsejusios-anksciau-nei-lietuvoje;
126. http://www.vkontrole.lt/page.aspx?id=15;
127. http://www.vuoi.lt/index.php?140866700;
128. https://www.epaslaugos.lt/portal/citizen/popular/services;
129. https://www3.cepol.europa.eu/dspace/bitstream/123456789/6752/1/Nedveckis.pdf;
130. http://www.axistech.com/WebPages/biometricexactedgrowth.aspx;
131. http://www.cl.cam.ac.uk;
132. http://www.sebio.com;
133. http://recogsys.com/index.shtml;
134. http://dir.salon.com/story/news/feature/2002/01/08/airport_security/index.html;
135. http://www.prweb.com/releases/2007/04/prweb516626.htm.

Šaltiniai rusų kalba:

136. Барковская Е. Г. Концепция создания криминалистических учетов на основе баз данных биометрии человека // Общество и право, 2009. № 1. С. 277-285.
137. Барковская Е. Г. Современные возможности использования биометрических данных человека в борьбе с преступностью // Использование достижения иных наук в

криминалистике: материалы Всерос. науч.-практ. конф. с международным участием / Кубанский государственный аграрный университет. - Краснодар, 2008. С. 13-17.

138. Биометрия идет в массы. 2012 // http://www.baltslon.ru/rus/publications/article242/; prisijungimo laikas: 2012-11-03.

139. Гинце А. Биометрические технологии в системах контроля и управления доступом // Системы безопасности, 2002. № 4. С. 50

140. Зайцев П.А. Практические вопросы выбора эффективной автоматизированной дактилоскопической идентификационной системы (АДИС) // Эксперт-криминалист, 2008. №2.

141. Каганов А. Ш. Криминалистическая идентификация личности по голосу и звучащей речи.− Юрлитинформ, 2009. Т. 1.

142. Краткая история биометрии. 2011 // http://www.tadviser.ru/index.php; prisijungimo laikas: 2012-10-01.

143. Куняев Н. Н. Проблема обеспечения защиты прав и свобод человека и гражданина в информационной сфере // Юридический мир, 2008. №9.

144. Курбатов С. Внедрение биометрических технологий идентификации личности − веяние времени. 2004 // http://www.comprice.ru/articles/detail.php?ID=40088; prisijungimo laikas: 2011-10-28.

145. Леонов В. П. История биометрики и ее применения // Международный журнал медицинской практики, 1999. В. 4.

146. Попов В. В., Сошников Е. А., Кистанов В. А. Современные средства видеоконтроля психофизиологических реакций обследуемого лица // Эксперт-криминалист, 2008. №2.

147. Степанов О. А. Проблема обеспечения общественной безопасности в условиях создания электронного государства // Государство и право, 2006. №1.

Trukšina O. Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybės užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje / Teisės ir policijos veiklos magistro baigiamasis darbas. Vadovas doc. dr. R. Vasiliauskas. – Kaunas: Mykolo Romerio universitetas, Viešojo saugumo fakultetas, 2013. – 98 p.

ANOTACIJA

Magistro baigiamajame darbe nagrinėjamos biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių problemos Lietuvos Respublikoje užtikrinant visuomenės saugumą ir viešąją tvarką.

Pirmajame darbo skyriuje atskleidžiama biometrijos ir biometrinių asmens tapatybės nustatymo sistemų samprata, nagrinėjama šių sistemų atsiradimo istorinės raidos tema. Nagrinėjami biometrinių asmens tapatybės nustatymo sistemų veikimo principai, šių sistemų panaudojimo galimybių pagrindai pasaulio šalyse užtikrinant visuomenės saugumą ir viešąją tvarką. Taip pat nagrinėjama biometrinių asmens tapatybės nustatymo sistemų panaudojimo poreikio tema Lietuvoje. Antrajame darbo skyriuje atskleidžiami tiriamos srities teisinio reglamentavimo Europos Sąjungoje ir Lietuvos Respublikoje pagrindiniai aspektai, analizuojamos pagrindinės asmens duomenų tvarkymo, naudojant biometrines asmens tapatybės nustatymo sistemas, teisinio reguliavimo problemos. Trečiasis darbo skyrius skirtas atskleisti visuomeninį požiūrį į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje, apibendrinami 2012-2013m. savarankiškai atlikto anketinio tyrimo gauti rezultatai. Darbo pabaigoje pateikiamos išvados ir pasiūlymai.

Pagrindiniai žodžiai: Biometrija, biometrinė sistema, biometrinis skaitytuvas, biometrinis požymis, biometrinis šablonas (modelis), asmens duomenys, asmens biometriniai duomenys.

Trukšina O. Possibilities of biometric personal identification establishment usage in ensuring public security and peace in the Republic of Lithuania / Master‘s Work in Law and Police Activities. Supervisor assoc. prof. dr. R. Vasiliauskas. – Kaunas: Faculty of Public Security, 2013. – 98 p.

ANOTATION

The Master thesis deals with the problems related to the application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace.

The paper consists of an introduction, three chapters, divided into separate subsections, conclusions and recommendations. Chapter one is designed to reveal the conception of biometrics and biometric personal identification systems as well as the historical development of these systems. The operational principles of biometric personal identification systems as well as the aspects of application of these systems in a number of countries for the ensurance of public security and peace are examined. The need of biometric personal identification systems in Lithuania is discussed. Chapter two discloses the main aspects of legal regulation of the field in question in the European Union and Lithuania, it analyses the main problems of the processing of personal biometric data by applying biometric identification systems. Chapter three is designed to reveal the social attitudes towards the application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace, the results of the questionnaire, which was independently carried out in 2012-2013, are taken into account. At the end of the paper, conclusions and recommendations are provided.

Key words: Biometrics, biometric system, biometric scanner, biometric characteristics, biometric template, personal data, personal biometric data.

Trukšina O. Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybės užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje / Teisės ir policijos veiklos magistro baigiamasis darbas. Vadovas doc. dr. R. Vasiliauskas. – Kaunas: Mykolo Romerio universitetas, Viešojo saugumo fakultetas, 2013. – 98 p.

SANTRAUKA

Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių problemos Lietuvoje užtikrinant visuomenės saugumą ir viešąją tvarką yra aktualios ir šios temos pasirinkimą lėmė asmens identifikacijos reikšmingumo augimas visame pasaulyje, o biometrinių asmens tapatybės nustatymo sistemų panaudojimas yra viena iš priemonių leidžiančių greitai, tiksliai ir efektyviai nustatyti asmens tapatybę.

Tyrimo hipotezė: Biometrinių asmens tapatybes nustatymo sistemų panaudojimas gali efektyviai padidinti visuomenės saugumo ir viešosios tvarkos užtikrinimo galimybes, tačiau jų praktinis įgyvendinimas Lietuvos Respublikoje nėra plačiai paplitęs.

Tyrimo objektas: Įvairių šalių mokslinių, teisinių ir praktinių pasiekimų tendencijos biometrinių asmens tapatybės nustatymo sistemų panaudojimo srityje užtikrinant visuomenės saugumą ir viešąją tvarką, šių tendencijų praktinio įgyvendinimo aspektai Lietuvos Respublikoje.

Tyrimo tikslas: Kompleksiškai išnagrinėti biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių aspektus užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje.

Tyrimo uždaviniai: 1) Išnagrinėti biometrinių asmens tapatybės nustatymo sistemų veikimo principus, šių sistemų panaudojimo aspektus įvairiose pasaulio šalyse užtikrinant visuomenės saugumą ir viešąją tvarką; 2) Nustatyti biometrinių asmens tapatybės nustatymo sistemų praktinio realizavimo galimybes ir pagrindinius biometrinių asmens duomenų tvarkymo teisinio reguliavimo aspektus Europos Sąjungoje ir Lietuvos Respublikoje; 3**)** Atskleisti visuomeninį požiūrį į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje; 4) Pateikti tyrimo išvadas ir pasiūlymus dėl biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje.

Tyrimo metodai: Tiriant biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybių, užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje,

probleminius aspektus bei perspektyvas yra taikomi šie tyrimo metodai: dokumentų analizės, lyginamasis istorinis, lyginamasis, loginis-analitinis, anketinis, matematinis statistinis.

Darbą sudaro įvadas, trys skyriai, kurie skirstomi į atskirus poskyrius, išvados ir pasiūlymai. Pirmasis darbo skyrius skirtas atskleisti biometrijos ir biometrinių asmens tapatybės nustatymo sistemų sampratą, šių sistemų atsiradimo istorinę raidą. Nagrinėjami biometrinių asmens tapatybės nustatymo sistemų veikimo principai, šių sistemų panaudojimo pagrindai pasaulio šalyse užtikrinant visuomenės saugumą ir viešąją tvarką. Nagrinėjama biometrinių asmens tapatybės nustatymo sistemų panaudojimo poreikio tema Lietuvoje. Antrajame darbo skyriuje atskleidžiami tiriamos srities teisinio reglamentavimo Europos Sąjungoje ir Lietuvoje pagrindiniai aspektai, analizuojamos pagrindinės asmens duomenų tvarkymo, naudojant biometrines asmens tapatybės nustatymo sistemas, teisinio reguliavimo problemos. Trečiasis darbo skyrius skirtas atskleisti visuomeninį požiūrį į biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybes užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje, apibendrinami 2012-2013m. savarankiškai atlikto anketinio tyrimo gauti rezultatai. Darbo pabaigoje pateikiamos išvados ir pasiūlymai.

Tyrimas parodė, kad biometrinių asmens tapatybės nustatymo sistemų panaudojimas gali efektyviai padidinti visuomenės saugumo ir viešosios tvarkos užtikrinimo galimybes, kaip rodo pasaulinė patirtis, tačiau jų praktinis įgyvendinimas Lietuvos Respublikoje nėra plačiai paplitęs dėl visuomenės neinformuotumo ir poreikio nebuvimo, o biometrinės sistemos pagrinde naudojamos tik tiek, kiek valstybė privalo, vykdydama teisines prievoles. Lietuvos Respublikoje galiojantys teisės aktai, susiję su biometrinių duomenų apsauga, iš esmės atitinka ES teisės aktuose keliamus reikalavimus, tačiau esami įstatymai Lietuvoje, reglamentuojantys asmens duomenų tvarkymą, nebuvo patikrinti biometrinių duomenų kontekste. Pagrindinės rizikos, galinčios atsirasti naudojant biometrines sistemas, yra asmens biometrinių duomenų neteisėtas naudojimas, biometrinių sistemų veikimo sutrikimai, galimas piktnaudžiavimas biometriniais duomenimis.

Trukšina O. Possibilities of biometric personal identification establishment usage in ensuring public security and peace in the Republic of Lithuania / Master's Work in Law and Police Activities. Supervisor assoc. prof. dr. R. Vasiliauskas. – Kaunas: Faculty of Public Security, 2013. – 98 p.

SUMMARY

The problems related to the application of biometric personal identification systems in Lithuania for the ensurance of public security and peace are relevant, and the chose of this investigation was determined by the growth of the importance to identify personalities around the entire world, meanwhile the application of biometric identification systems is one of the means allowing quick, accurate and efficient identification of personalities.

Research hypothesis: The application of biometric identification systems can effectively increase the opportunities to ensure public security and peace, however, their practical implementation is not widespread in Lithuania.

Research object: Scientific, legal and practical achievements of various countries in the practical application of biometric personal identification systems for the ensurance of public security and peace, the trends of practical implementation of these achievements in the Republic of Lithuania.

Research aim: To comprehensively investigate the aspects of practical application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace.

Research objectives: 1) To analyze the operational principles of biometric personal identification systems as well as the aspects of application of these systems in a variety of countries for the ensurance of public security and peace; 2) To determine the opportunities of practical realization of biometric personal identification systems and the main legal aspects of the processing of personal biometric data in the European Union and the Republic of Lithuania; 3) To reveal the social attitude towards the application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace; 4) To provide research conclusions and recommendations for the application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace.

Research methods: For the analysis of the problemic aspects and prospects of the application of biometric personal identification systems in the Republic of Lithuania for the

ensurance of public security and peace, the following methods were applied: document analysis, comparative-historical method, comparative method, logical-analytical method, questionnaire, mathematical statistics.

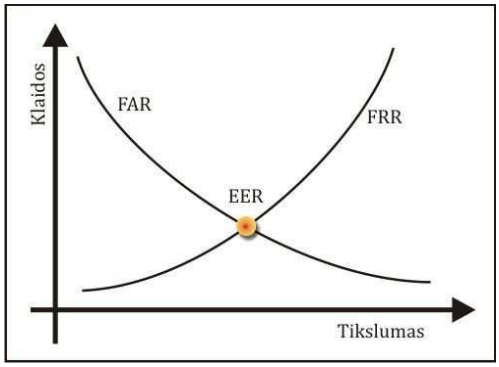
The paper consists of an introduction, three chapters, divided into separate subsections, conclusions and recommendations. Chapter one is designed to reveal the conception of biometrics and biometric personal identification systems as well as the historical development of these systems. The operational principles of biometric personal identification systems as well as the aspects of application of these systems in a number of countries for the ensurance of public security and peace are examined. The need of biometric personal identification systems in Lithuania is discussed. Chapter two discloses the main aspects of legal regulation of the field in question in the European Union and Lithuania, it analyses the main problems of the processing of personal biometric data by applying biometric identification systems. Chapter three is designed to reveal the social attitudes towards the application of biometric personal identification systems in the Republic of Lithuania for the ensurance of public security and peace, the results of the questionnaire, which was independently carried out in 2012-2013, are taken into account. At the end of the paper, conclusions and recommendations are provided.

The research has showed that the application of biometric personal identification systems can effectively increase the public security and peace, as evidenced by the global experiences, however, their practical implementation is not widespread in Lithuania due to the public unawareness and the absence of the need, and biometric systems are mainly used only to an extent the state is obliged to use them in the implementation of its legal commitments. The existing legislation of the Republic of Lithuania related to the security of biometric data is broadly in line with EU legislative requirements, however, the existing laws of the Republic of Lithuania regulating the processing of personal data were not verified in the context of biometric data. The main risks that may arise from the application of biometric systems are the illegal use of personal biometric data, malfunction of biometric systems and the possible misuse of biometric data.

P R I E D A I

1 PRIEDAS

KLAIDOS GALIMYBĖS PRIKLAUSOMYBĖ NUO TIKSLUMO



Šaltinis: Stan Z. Li, Anil K. Jain . Enciplopedia of biometrics.- Springer, 2009. P. 192.

1 pav. Klaidos galimybės priklausomybė nuo tikslumo

Neteisingo priėmimo galimybė (*angl. False Acceptance Rate (FAR*)) – tikimybė, kad biometrinė sistema svetimą žmogų atpažins kaip savą.

Neteisingo atmetimo galimybė *(angl. False Rejection Rate (FRR))* – tikimybė, reiškia kad registruotas vartotojas bus neatpažintas ir reikės dar kartą nuskaityti asmens duomenis.

Bendrą klaidos galimybė *(alng Equal Error Rate (EER))* – FAR ir FRR verčių „aukso vidurys".

2 PRIEDAS

BIOMETRINIŲ POŽYMIŲ SULYGINIMAS PAGAL BENDRUS KRITERIJUS

1 lentelė. Biometrinių požymių sulyginimas pagal bendrus kriterijus

Biometrinis požymis (metodas)	**Bendri kriterijai**							
	Universalumas	Unikalumas	Permanentiškumas	Pamatuojamumas	Atsparumas aplinkos faktoriams	Tikslumas	Atsparumas klastojimui	Socialinis priimtinumas
Piršto atspaudai	**V**	**A**	**A**	**V**	**Ž**	**A**	**V**	**V**
Delno atspaudai	**V**	**A**	**A**	**V**	**V**	**A**	**A**	**V**
Delno geometrija	**V**	**V**	**V**	**A**	**V**	**V**	**V**	**V**
Delno kraujagyslės	**V**	**V**	**V**	**V**	**V**	**V**	**A**	**A**
Akies rainelė	**A**	**A**	**A**	**V**	**V**	**A**	**A**	**Ž**
Akies tinklainė	**A**	**A**	**V**	**Ž**	**A**	**A**	**A**	**Ž**
Veidas dvimatis	**A**	**Ž**	**V**	**A**	**Ž**	**V**	**V**	**A**
Veidas trimatis	**A**	**V**	**V**	**V**	**V**	**V**	**A**	**A**
Veido termograma	**A**	**A**	**Ž**	**A**	**V**	**V**	**A**	**A**

Ausies geometrija	**V**	**V**	**A**	**V**	**V**	**A**	**V**	**A**
Kvapas	**A**	**A**	**A**	**Ž**	**Ž**	**Ž**	**Ž**	**V**
Genetinio kodo fragmentai	**A**	**A**	**A**	**V**	**A**	**A**	**A**	**V**
Eisena	**V**	**Ž**	**Ž**	**A**	**Ž**	**A**	**V**	**A**
Darbas su klaviatūra	**Ž**	**Ž**	**Ž**	**V**	**Ž**	**V**	**V**	**V**
Parašas	**Ž**	**Ž**	**Ž**	**A**	**A**	**V**	**Ž**	**Ž**

Šaltinis: Stupak V., Vasiliauskas R. Biometrinių atpažinimo sistemų efektyvumo nagrinėjimo informatikos studijose aspektai // Policijos pareigūnų profesinio rengimo aktualijos. Mokslinių straipsnių rinkinys. – Kaunas: Mykolo Romerio universiteto Viešojo saugumo fakultetas, 2007. P. 87 – 88.

A – aukštas atitikimo laipsnis, **V** – vidutinis atitikimo laipsnis, **Ž** – žemas atitikimo laipsnis.

3 PRIEDAS

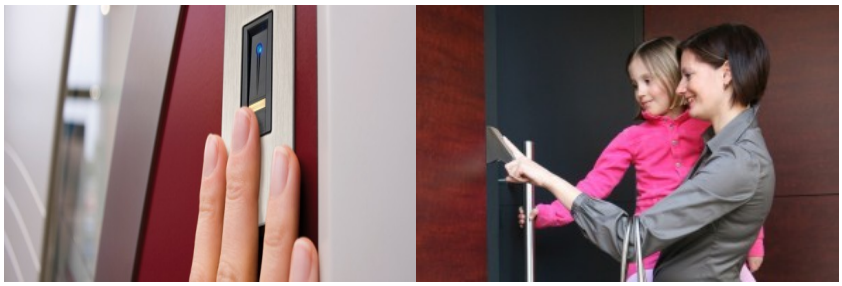
KAI KURIŲ BIOMETRINIŲ ASMENS TAPATYBĖS NUSTATYMO SISTEMŲ PAVYZDŽIAI

Biometrinės sistemos bankomatuose naudojamos klientų identifikavimui. Tokios biometrinės sistemos atpažįsta asmenį, pvz., pagal rankos pirštų atspaudus, veninių kraujagyslių sistemos išsidėstymą išoriniame delno paviršiuje ir pan.

Šaltinis: *http://www.technologijos.lt/n/technologijos/technologiju_rinka/S-25566/straipsnis/Japonijos-bankas-naudos-visiskai-biometrinius-bankomatus?l=2&p=1*

1 pav. Biometrinė sistema bankomate

Naudojant **biometrines elektronines spynas**, vartotojui perbraukus pirštu per biometrinį skaitytuvą, gauti duomenys paverčiami šablonu (modeliu) ir išsaugomi duomenų bazėje kaip unikalus raktas. Kiekvieną kartą, nuskaitant piršto antspaudus, duomenys konvertuojami į kodą ir palyginami su duomenų bazėje esančiu šablonu (modeliu). Tik tada kai duomenys sutampa, gaunamas leidimas pateikti į patalpas.



Šaltinis: *http://www.elektroninesspynos.lt/biometrines-elektronines-spynos-kas-tai/*

2 pav. Biometrinė elektroninė spyna

3 priedo tęsinys

Biometrinės sistemos įdiegtos kompiuteriuose apsaugo nuo svarbių duomenų praradimo, konfidencialios informacijos paviešinimo, informacijos pasisavinimo, duomenų vagystės ir t. t.

Šaltinis: *http://www.houseofjapan.com/electronics/fujitsu-5mm-thick-palm-vein-sensor-small-enough-to-fit-on-a-tablet*

3 pav. Biometrinės sistemos kompiuteriuose

Biometrinės įėjimo kontrolės sistemos skirtos kontroliuoti asmenų patekimą į ypač didelio saugumo patalpas: pinigų saugyklas, valstybines institucijas ir t.t.

Šaltiniai: *http://www.ucs.lt/sprendimai/kita/biotime;*

http://www.channelprosmb.com/article/biometric-security-solution-replaces-passwords-with-palm-scan

4 pav. Daugiarūšės biometrinės įėjimo kontrolės sistemos

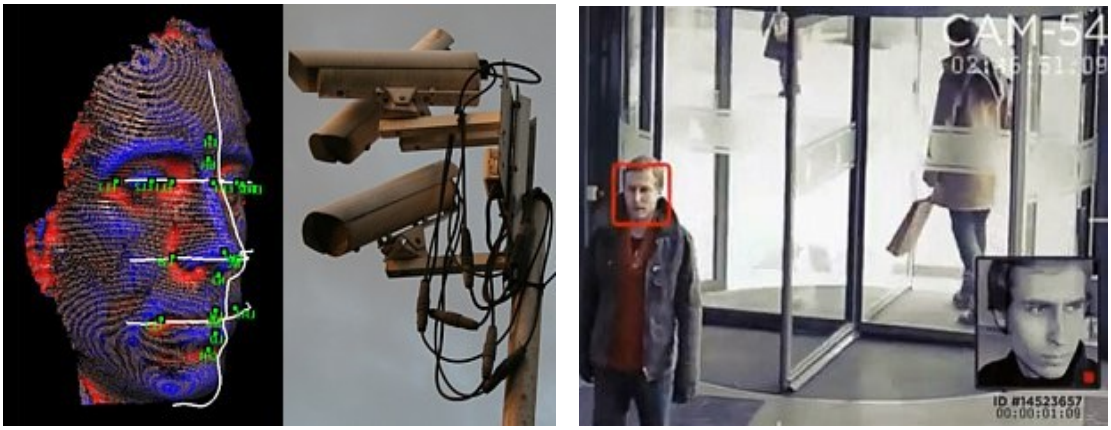
3 priedo tęsinys

Biometrinės sistemos oro uostuose supaprastina keleivių registracijos, bagažo patikrinimo, įlaipinimo ir pasų kontrolės procesus.

Šaltinis: *http://vilnius.usembassy.gov/kelioniu-supaprastinimo-programa.html*

5 pav. Biometrinė sistema oro uoste. Asmens atpažinimas pagal akies rainelės piešinį

Biometrinių veido atpažinimo sistemų naudojimas masinio susibūrimo vietose, oro ir jūros uostuose, stotyse, dideliuose prekybos centruose padeda greitai ir tiksliai nustatyti ir surasti įtariamuosius, kitus asmenis, kuriems įstatymų nustatyta tvarka paskelbta paieška.



Šaltinis: *http://pinktentacle.com/2007/07/necs-drive-thru-face-recognition-system/*

6 pav. Biometrinė veido atpažinimo sistema

4 PRIEDAS

ANKETŲ PAVYZDŽIAI

ANKETA KRMINALINĖS POLICIJOS SKYRIŲ TYRĖJAMS IR JŲ VADOVAMS

Gerb. Kolege!
Prašome atsakyti į anketos klausimus. Rezultatai reikalingi empiriniam tyrimui atlikti magistro darbe
„**Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybės užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje**“ .
Anketa yra anonimiška.

Atsakymą prašome pažymėti ženklu „ X ”

Klausimai	Atsakymai		
	Taip	**Ne**	**Nežinau**
1. Ar Jums yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos (ADIS) galimybes atskleidžiant ir tiriant nusikalstamas veikas?			
2. Ar Jums yra žinoma apie DNR duomenų registro įsteigimą ir galimybes atskleidžiant ir tiriant nusikalstamas veikas?			
3. Ar ADIS ir (ar) DNR registro duomenų panaudojimas padėjo atskleisti ir tirti nusikalstamas veikas Jūsų žinioje esančiose ikiteisminio tyrimo medžiagose?			
4. Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą?			
5. Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą?			
6. Ar Jums yra žinoma kaip (kokiu pavidalu) yra saugojami asmens biometriniai duomenys?			
7. Ar galėtumėte nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie galėtų būti panaudojami biometrinėse asmens tapatybės nustatymo sistemose (toliau BATNS?)			
8. Ar Jums yra žinoma, kokios BATNS ir kokiose srityse yra naudojamos plačiausiai užsienio šalyse?			
9. Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją?			
10. Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą?			
11. Ar galėtų, Jūsų nuomone, BATNS padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas (pvz. oro uostuose, bankuose, stadionuose, masinio susibūrimo vietose, elektroninės bankininkystės sistemose kt.)?			

4 priedo tęsinys

12. Ar, Jūsų nuomone, Europos Sąjungoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?			
13. Ar, Jūsų nuomone, Lietuvoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?			
14. Ar , Jūsų nuomone, yra pakankamai literatūros lietuvių kalba (moksliniai, mokslo populiarinimo straipsniai, knygos) apie BATNS ir jų panaudojimo galimybes?			

Ačiū už dalyvavimą !

4 priedo tęsinys

ANKETA INTERNETE

Gerb. Lankytojau!
Prašome atsakyti į anketos klausimus. Rezultatai reikalingi empiriniam tyrimui atlikti magistro darbe
„**Biometrinių asmens tapatybės nustatymo sistemų panaudojimo galimybės užtikrinant visuomenės saugumą ir viešąją tvarką Lietuvos Respublikoje**“
Ačiū už dalyvavimą !

---

1. Ar Jums yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos (ADIS) galimybes atskleidžiant ir tiriant nusikalstamas veikas?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
2. Ar Jums yra žinoma apie DNR duomenų registro įsteigimą ir galimybes atskleidžiant ir tiriant nusikalstamas veikas?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
3. Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
4. Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
5. Ar Jums yra žinoma kaip (kokiu pavidalu) yra saugojami asmens biometriniai duomenys?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
6. Ar galėtumėte nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie galėtų būti panaudojami biometrinėse asmens tapatybės nustatymo sistemose (toliau BATNS?)

1. taip

2. ○ ne
3. ○ nežinau

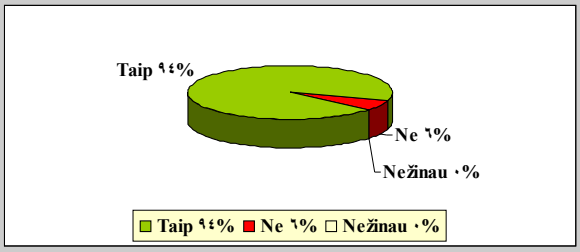
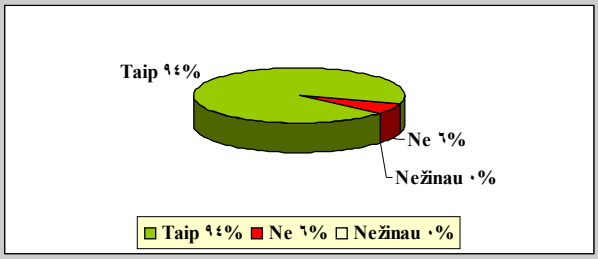
7. Ar Jums yra žinoma, kokios BATNS ir kokiose srityse yra naudojamos plačiausiai užsienio šalyse?
   1. ○ taip
   2. ○ ne
   3. ○ nežinau
8. Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją?
   1. ○ taip
   2. ○ ne
   3. ○ nežinau
9. Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą?
   1. ○ taip
   2. ○ ne
   3. ○ nežinau
10. Ar galėtų, Jūsų nuomone, BATNS padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas (pvz. oro uostuose, bankuose, stadionuose, masinio susibūrimo vietose, elektroninės bankininkystės sistemose kt.)?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
11. Ar, Jūsų nuomone, Europos Sąjungoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau
12. Ar, Jūsų nuomone, Lietuvoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?
    1. ○ taip
    2. ○ ne
    3. ○ nežinau

Siųsti atsakymą

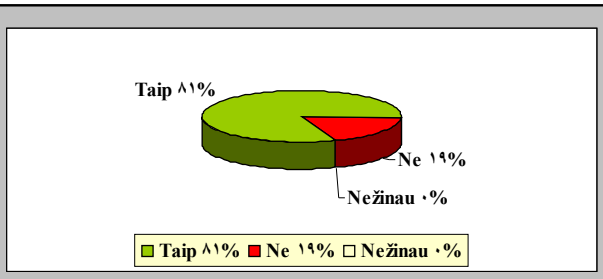
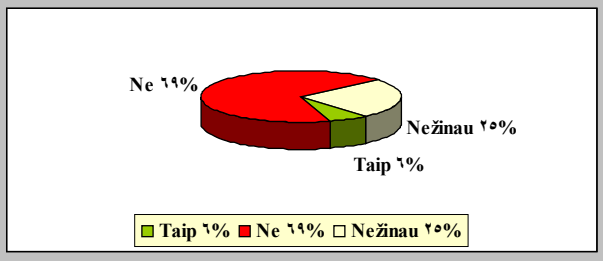
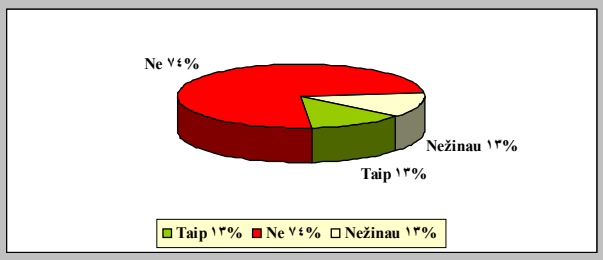
5 PRIEDAS

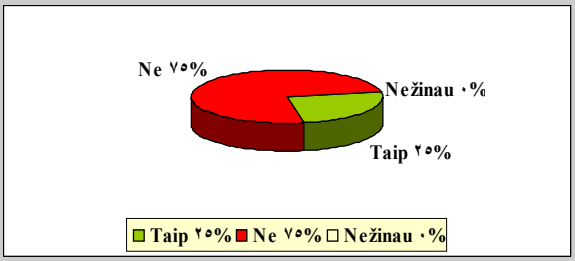
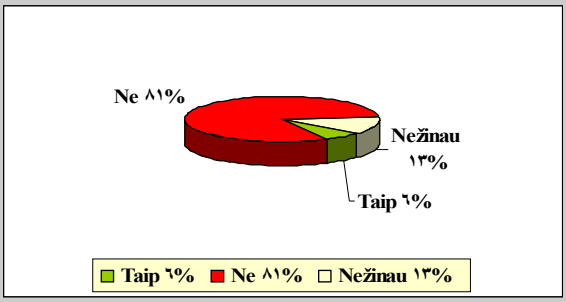
APKLAUSOS REZULTATAI

Kriminalinės policijos skyrių tyrėjų ir jų vadovų apklausos rezultatai

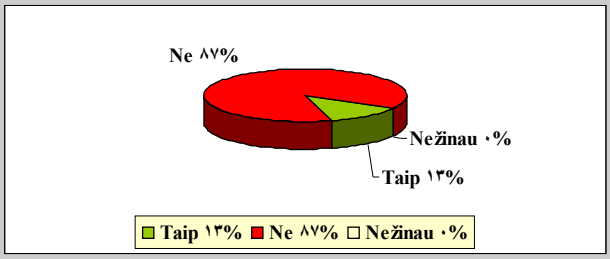
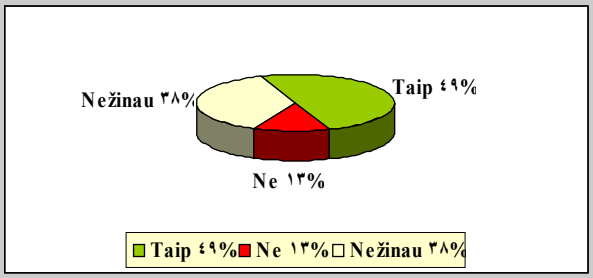
Atsakymų į klausimus grafiniai paveikslai	Atsakymų kiekis ir santykis		
	Taip	Ne	Nežinau
 **1 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos (ADIS) galimybes atskleidžiant ir tiriant nusikalstamas veikas?”	90 93,75%	6 6,25%	0
 **2 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma apie DNR duomenų registro įsteigimą ir galimybes atskleidžiant ir tiriant nusikalstamas veikas? ”	90 93,75%	6 6,25%	0

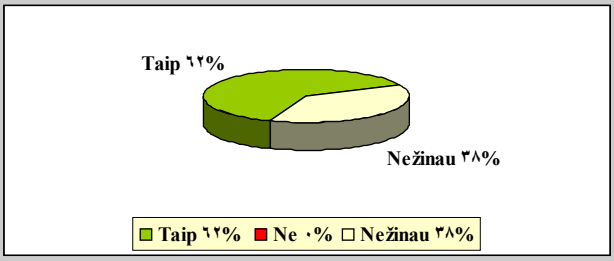
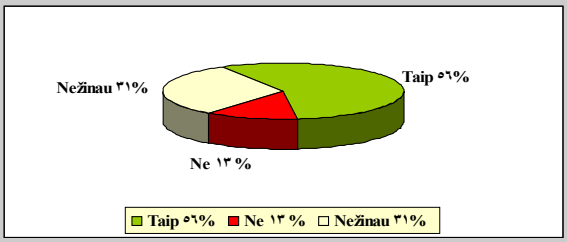
5 priedo tęsinys

 **3 pav.** Atsakymai į klausimą ,,Ar ADIS ir (ar) DNR registro duomenų panaudojimas padėjo atskleisti ir tirti nusikalstamas veikas Jūsų žinioje esančiose ikiteisminio tyrimo medžiagose?”	**78** **81,25%**	**18** **18,75%**	**0**
 **4 pav. Atsakymai į klausimą „**Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą?”	**6** **6,25%**	**66** **68,75%**	**24** **25%**
 **5 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą?”	**12** **12,5%**	**72** **75%**	**12** **12,5%**

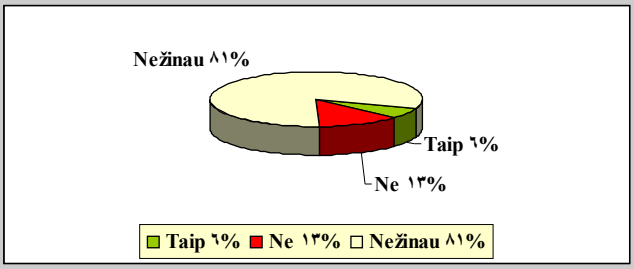
 **6 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma kaip (kokiu pavidalu) yra saugojami asmens biometriniai duomenys?”	**24** **25%**	**72** **75%**	**0**
 **7 pav.** Atsakymai į klausimą ,,Ar galėtumėte nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie galėtų būti panaudojami biometrinėse asmens tapatybės nustatymo sistemose (toliau BATNS?)”	**6** **6,25%**	**78** **81.25%**	**12** **12,5%**

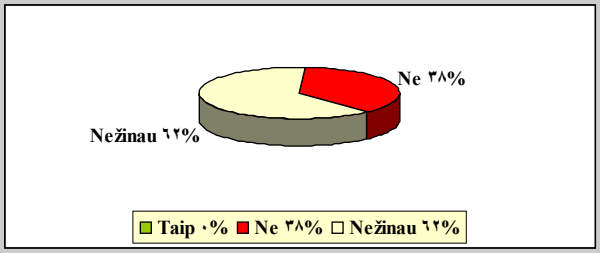
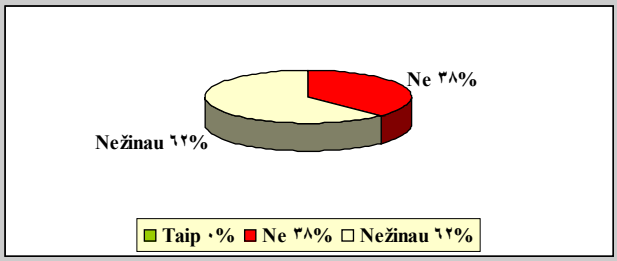
5 priedo tęsinys

 **8 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma, kokios BATNS ir kokiose srityse yra naudojamos plačiausiai užsienio šalyse?”	**12** **12,5%**	**84** **87,5%**	**0**
 **9 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją?”	**48** **50%**	**12** **12,5%**	**36** **37,5%**

 **10 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą?”	**60** **62,5%**	**0**	**36** **37,5%**
 **11 pav. Atsakymai į klausimą** ,,Ar galėtų, Jūsų nuomone, BATNS padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas (pvz. oro uostuose, bankuose, stadionuose, masinio susibūrimo vietose, elektroninės bankininkystės sistemose kt.)?”	**54** **56,25%**	**12** **12,5%**	**30** **31,25%**

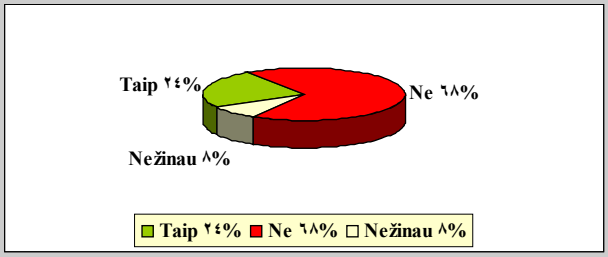
5 priedo tęsinys

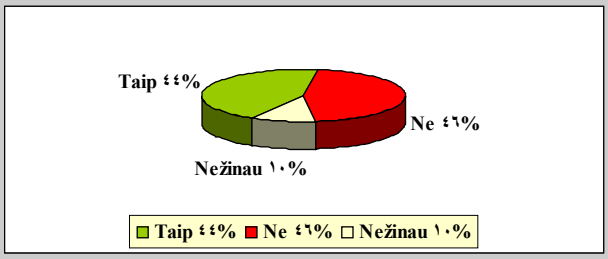
 **12 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, Europos Sąjungoje yra	**6** **6,25%**	**12** **12,5%**	**78** **81,25%**

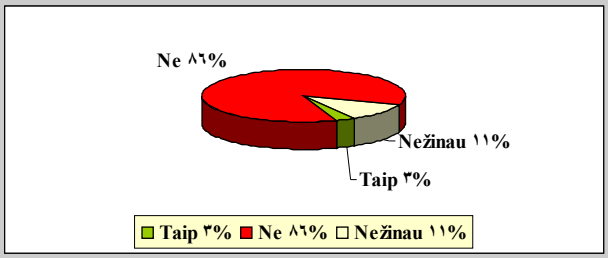
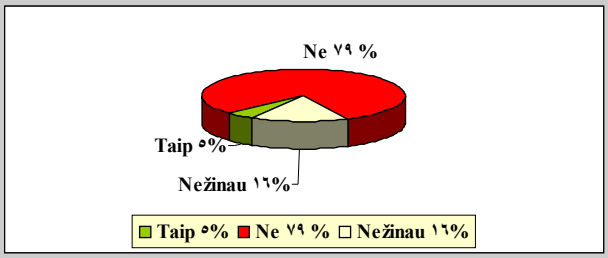
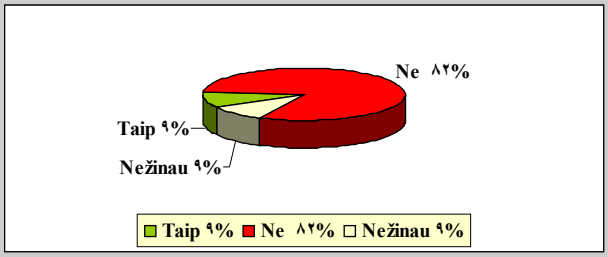
sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?”			
 **13 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, Lietuvoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?”	**0**	**36 37,5%**	**60 62,5%**
 **14 pav. Atsakymai į klausimą** ,,Ar , Jūsų nuomone, yra pakankamai literatūros lietuvių kalba (moksliniai, mokslo populiarinimo straipsniai, knygos) apie BATNS ir jų panaudojimo galimybes?”	**0**	**36 37,5%**	**60 62,5%**

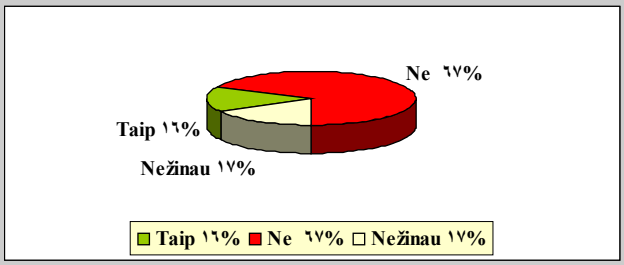
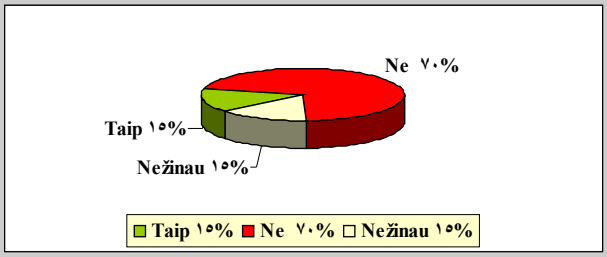
5 priedo tęsinys

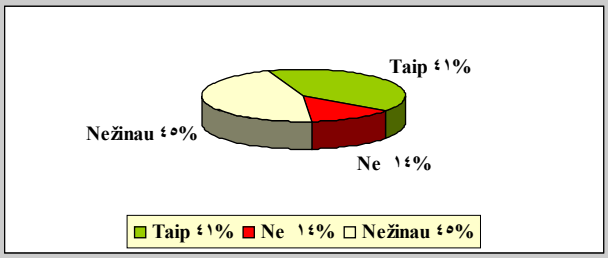
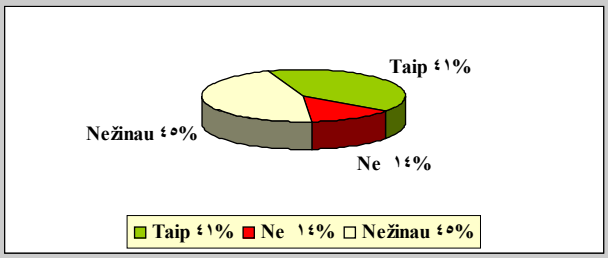
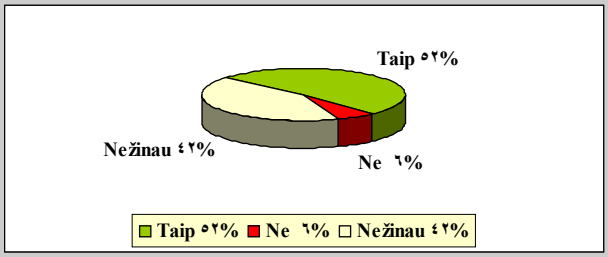
Apklausos rezultatai internetinėje svetainėje www.apklausa.lt

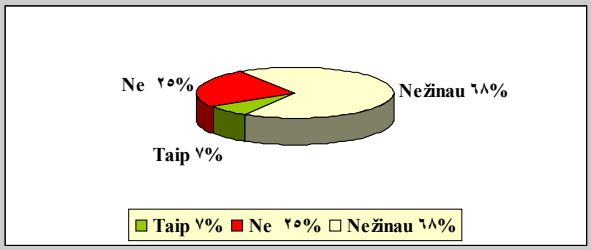
Atsakymų į klausimus grafiniai paveikslai	Atsakymų kiekis ir santykis		
	Taip	Ne	Nežinau
 **15 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma apie automatizuotos daktiloskopinės identifikavimo sistemos (ADIS) galimybes atskleidžiant ir tiriant nusikalstamas veikas?”	23 24%	65 67,7%	8 8,3%

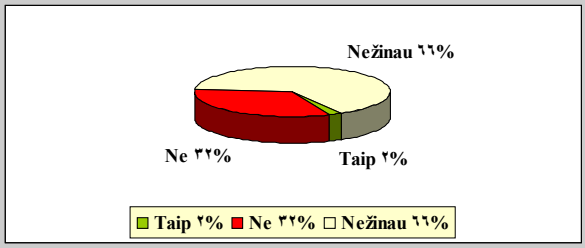
 **16 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma apie DNR duomenų registro įsteigimą ir galimybes atskleidžiant ir tiriant nusikalstamas veikas?”	42 43,8%	44 45,8%	10 10,4%

 **17 pav. Atsakymai į klausimą „**Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens biometrinių duomenų patikimumą ir šios informacijos saugojimo būdą?”	**3** **3,1%**	**82** **85,4%**	**11** **11,5%**
 **18 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, visuomenė Lietuvoje yra pakankamai informuojama apie asmens tapatybę patvirtinančių dokumentų su biometriniais duomenimis patikimumą ir saugumą?”	**5** **5,2%**	**75** **78,1%**	**16** **16,7%**
 **19 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma kaip (kokiu pavidalu) yra saugojami asmens biometriniai duomenys?”	**9** **9,4%**	**78** **81,2%**	**9** **9,4%**

 **20 pav.** Atsakymai į klausimą ,,Ar galėtumėte nurodyti 10 unikalių žmogaus fizinių požymių ir elgesio savybių, kurie galėtų būti panaudojami biometrinėse asmens tapatybės nustatymo sistemose (toliau BATNS?)”	**15** **15,6 %**	**65** **67,7 %**	**16** **16,7 %**
 **21 pav.** Atsakymai į klausimą ,,Ar Jums yra žinoma, kokios BATNS ir kokiose srityse yra naudojamos plačiausiai užsienio šalyse?”	**14** **14,6 %**	**68** **70,8 %**	**14** **14,6 %**

 **22 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti nusikalstamų veikų prevenciją?”	**39** **40,6 %**	**13** **13,5%**	**44** **45,9%**
 **23 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, BATNS panaudojimas Lietuvoje galėtų užtikrinti efektyvų nusikalstamų veikų atskleidimą ir tyrimą? ”	**50** **52,1%**	**6** **6,2%**	**40** **41,7%**
 **24 pav. Atsakymai į klausimą** ,,Ar galėtų, Jūsų nuomone, BATNS padėti užtikrinti visuomenės saugumą ir viešąją tvarką kontroliuojant įėjimą į fizines ir virtualias zonas (pvz. oro uostuose, bankuose, stadionuose, masinio susibūrimo vietose, elektroninės bankininkystės sistemose kt.)?”	**50** **52,1%**	**6** **6,2%**	**40** **41,7%**

 **25 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, Europos Sąjungoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?”	**7** **7,3%**	**24** **25%**	**65** **67,7%**

 **26 pav.** Atsakymai į klausimą ,,Ar, Jūsų nuomone, Lietuvoje yra sukurta pakankama teisinė bazė, reglamentuojanti BATNS panaudojimą teisėtvarkoje ir visuomeniniame gyvenime?”	**2** **2,1%**	**31** **32,3%**	**63** **65,6%**