

**MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS**

EDGARAS SRIUBAS

**BIOMETRINIŲ TECHNOLOGIJŲ PLĖTROS
GRĖSMĖS ASMENS DUOMENŲ APSAUGAI**

Magistro baigiamasis darbas

**Vadovas
doc. dr. Marius Laurinaitis**

VILNIUS, 2023

**MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS**

**BIOMETRINIŲ TECHNOLOGIJŲ PLĖTROS
GRĖSMĖS ASMENS DUOMENŲ APSAUGAI**

**Viešojo valdymo ir verslo magistro baigiamasis darbas
Studijų programa 6211LX066**

**Konsultantas
(parašas)
2023 - -**

**Vadovas
(parašas) doc. dr. M. Laurinaitis
2023 - -**

**Recenzentas
(parašas)
2023 - -**

**Atliko
KSV-vmis21-1 gr. stud.
(parašas) E. Sriubas
2023 - -**

VILNIUS, 2023

TURINYS

LENTELĖS	4
PAVEIKSLAI	5
SANTRUMPOS	6
ĮVADAS.....	7
1. BIOMETRINIŲ TECHNOLOGIJŲ PLĖTROS GRĖSMĖS TEORINIAI ASPEKTAI.....	10
1.1. Biometrinių technologijų samprata ir koncepcija	10
1.2. Biometrinės technologijos ir jų veikimo principas	13
1.3. Biometrinių technologijų plėtra	21
1.4. Biometrinių technologijų sąlygojamos grėsmės	22
1.4.1. Grėsmių sritys	22
1.4.2. Atakos biometrinėse sistemose	24
1.4.3. Grėsmės privatumą išsaugančioms biometrinėms autentifikavimo sistemoms	26
1.5. Asmens duomenų apsaugos reglamentavimas	30
1.6. Biometrikos ir kibernetinio saugumo standartai	32
2. TYRIMAI ATLIKTI BIOMETRINIŲ TECHNOLOGIJŲ NAUDOJIMO KONTEKSTE	35
2.1. Šalių reitingavimas pagal biometrinių duomenų rinkimą ir panaudojimą	35
2.2. Biometrinių duomenų ir elgsenos masinė stebėsena ES valstybėse narėse	37
2.3. Biometrikos instituto metinė pramonės apklausa.....	39
2.4. Deepfake technologijos grėsmės biometrinėms sistemoms	40
3. LIETUVOS VARTOTOJŲ POŽIŪRIO Į BIOMETRINES TECHNOLOGIJAS IR ASMENS DUOMENŲ SAUGUMĄ TYRIMO METODOLOGIJA	42
3.1. Tyrimo metodika	42
3.2. Ekspertų interviu	43
4. LIETUVOS VARTOTOJŲ POŽIŪRIO Į BIOMETRINES TECHNOLOGIJAS IR ASMENS DUOMENŲ SAUGUMĄ EMPIRINIO TYRIMO REZULTATAI.....	47
4.1. Biometrinių technologijų įtaka asmens duomenų saugumui ir privatumui.....	47
4.2. Etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims.....	50
4.3. Vartotojų švietimo ir informuotumo didinimo kampanijos	54
4.4. Pamonės savireguliacija ir jos vaidmuo.....	55

4.5. Biometrinių technologijų ateitis	56
4.6. Lietuvos vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą tyrimo rezultatai	57
4.7. Biometrinių technologijų plėtros atsparumo grėsmėms modelis, atsižvelgiant į tyrimo rezultatus	70
IŠVADOS IR REKOMENDACIJOS	74
LITERATŪRA.....	76
ANOTACIJA	81
ANNOTATION	82
SANTRAUKA	83
SUMMARY	84
PRIEDAI	85
Priedas 1. tyrime naudota anketa.....	85
Priedas 2. tyrime naudota anketa.....	87
Priedas 3. Patvirtinimas apie atlikto darbo savarankiškumą	91

LENTELĖS

1 lentelė. Įvairių biometrinių metodų palyginimas pagal savybes	12
2 lentelė. Biometrinių technologijų plėtros grėsmių atsparumo asmens duomenų apsaugai Lietuvoje modelis	71

PAVEIKSLAI

1 pav. Autentifikavimo sistemų atakos	28
2 pav. Biometrinių duomenų rinkimo ir saugojimo pagal šalis žemėlapis	36
3 pav. Ekspertų grupės dydžio poveikis patikimumui	43
4 pav. Ekspertų anketos sudarymo nuoseklumas	44
5 pav. Amžiaus pasiskirstymas	57
6 pav. Išsilavinimo laipsnio pasiskirstymas	58
7 pav. Susipažinimas su biometrinėmis technologijomis.....	58
8 pav. Biometrinių technologijų naudojimo pasiskirstymas	59
9 pav. Biometrinės technologijų įrenginiuose naudojimas	59
10 pav. Biometrinių technologijų saugumo palyginimas su tradicinėmis tapatybės nustatymo priemonėmis.....	60
11 pav. Tapatybės patvirtinimo priemonių pirmenybės teikimo pasiskirstymas	60
12 pav. Biometrinių duomenų rinkimo, saugojimo ir naudojimo kontrolės svarba.....	61
13 pav. Pagrindinės rizikos biometrinių technologijų naudojimo kontekste	61
14 pav. Nuomonė biometrinių technologijų naudojimo asmens duomenų rinkimui ir tvarkymui kontekste.....	62
15 pav. Iššūkiais ir rizikos veiksniais siejami su biometrinėmis technologijomis Lietuvoje	62
16 pav. Nuomonė, dėl viešojo ir privataus sektoriaus įmonių privalomo vertinimo	63
17 pav. Nuomonė, dėl įmonių asmens duomenų tvarkymo praktikos viešinimo	64
18 pav. Pasitikėjimas įmonių tinkamu asmens duomenų saugojimu	64
19 pav. Galimybė kontroliuoti savo biometrinių duomenų naudojimą.....	65
20 pav. Biometrinių technologijų naudojimas viešojoje erdvėje	65
21 pav. Informacijos ir švietimo poreikis biometrinių technologijų naudojimo kontekste	66
22 pav. Nuomonė, dėl didesnių įkainių taikymo produktams ar paslaugoms, naudojančioms saugesnes biometrinės technologijas.....	66
23 pav. Vartotojų teisių apsauga biometrinių technologijų naudojimo srityje	67
24 pav. Pasitenkinimo lygis naudojantis biometrinėmis technologijomis	67
25 pav. Nerimas, dėl galimybių biometrinius duomenis perduoti trečiosioms šalims.....	68
26 pav. Susipažinimas su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą	68
27 pav. Susidūrimas su asmens duomenų vagystės atvejais	69
28 pav. Susidūrimas su biometrinių technologijų klaidomis ar trūkumų atvejais	69
29 pav. Rizikos valdymo priemonių modelis.....	72

SANTRUMPOS

BDAR – Bendrasis duomenų apsaugos reglamentas

CCPA (angl. *California Consumer Privacy Act*) – Kalifornijos vartotojų privatumo įstatymas

COVID-19 (angl. *Coronavirus disease 2019*) – Koronaviruso liga 2019

DAP – Duomenų apsaugos pareigūnas

DI – Dirbtinis intelektas

EB – Europos Parlamento ir Tarybos reglamentas

ES – Europos Sąjunga

EU (angl. *The European Union*) – Europos Sąjunga

FAR (angl. *False Acceptance Rate*) – Klaidingo priėmimo rodiklis

FIDO2 (angl. *Fast Identity Online 2*) – Greito tapatybės nustatymo internetu antrasis standartas

FRR (angl. *False Rejection Rate*) – Klaidingo atmetimo rodiklis

GDPR (angl. *General data protection*) – Bendrasis duomenų apsaugos reglamentas

IEC (angl. *International Electrotechnical Commission*) – Tarptautinė elektrotechnikos komisija

ISO (angl. *International Organization for Standardization*) – Tarptautinė standartizacijos organizacija

IT – Informacinės technologijos

JAV – Jungtinės Amerikos Valstijos

NFC (angl. *Near Field Communication*) – Artimojo lauko komunikacija

NIST (angl. *National Institute of Standards and Technology*) – Nacionalinis standartų ir technologijų institutas

PAD (angl. *Presentation attack determination*) – Pateikimo atakos nustatymas

PIN (angl. *Personal identification number*) – Asmens identifikacinis numeris

RBI (angl. *Remote biometric identification*) – Nuotolinis biometrinis identifikavimas

RFID (angl. *Radio frequency identification*) – Radijo dažnio identifikavimas

IVADAS

Temos aktualumas ir teorinis reikšmingumas. Biometrinės technologijos šiuo metu yra aktuali tema, kuri turi didelę teorinę svarbą šių dienų kontekste, vykstanti technologijų plėtra, atveria terpę potencialioms grėsmėms įtakojančioms asmens duomenų saugumą ir privatumą. Biometriniai duomenys pasižymi unikalumu ir nekintamumu, ko pasėkoje kompromitacijos atveju, atsiranda negrįžtama tam tikrų grėsmių, bei pavojų tikimybė. Tai reiškia, kad šių duomenų nesankcionuotas panaudojimas, potencialiems nusikaltėliams, suteikia prieigą prie asmens duomenų, kaip ir suteikia galimybes juos panaudoti kenkėjiškais tikslais. Sparti technologijų plėtra, reikalauja didinti visuomenės supratimą, kaip yra naudojami biometriniai duomenys, kokie saugumo mechanizmai šiose sistemose yra taikomi, koku būdu užtikrinamas asmens duomenų privatumas ir kokia viso to sąlygojama nauda. 2019 m. rugpjūčio mėn. autorių Noam Rotem ir Ran Locar, paskelbtoje „Vpnmentor“ saugumo tyrimų ataskaitoje yra atskleidžiamas didelis Jungtinių Karalysčių „Metropoliteno policijos“, bankų ir gynybos rangovų naudojamos biometrinės sistemos pažeidimo mastas, kuomet nutekėjo duomenų bazės duomenys. Incidento padariniai, apėmė daugiau nei milijono gyventojų asmens duomenų paviešinimą, tarp kurių buvo ir biometriniai duomenys. Viešai buvo paviešinti veido atpažinimo įrašai, pirštų atspaudai, veiklos žurnalų duomenimis ir kita asmeninė informacija. Tai parodė, jog netinkamas asmens duomenų saugojimas ir saugumo užtikrinimas, vartotojams gali sukelti nepataisomą žalą. Vykstant šių technologijų plėtrai privatūs ir viešieji subjektai, vis dažniau diegia įvairius išmanaus stebėjimo sprendimus. Tarp taikomų sprendimų naudojamas ir nuotolinis biometrinis identifikavimas, kuris gali būti grystas veido atpažinimo algoritmais ar kitais biometrinių technologijų metodais. Tokių sistemų taikymas, suteikia galimybes biometrinius duomenis rinkti automatiniu būdu, be asmens žinios, ar sutikimo suteikimo. Tai reiškia, kad tokios metodikos taikymas, duomenų rinkimui, gali būti neteisėtas ir prieštarauti asmens duomenų apsaugos teisėms. Neteisėtas biometrinių duomenų rinkimas gali pasireikšti ir kitomis formomis socialiniuose tinkluose viešinamos nuotraukos gali būti pasitelkiamos dirbtinių intelekto (DI) algoritmų apmokymams. Ko pasėkoje gali būtų imituojami realūs asmenys, siekiant juos kompromituoti, ar taip išgauti realios naudos. Visa tai yra tik dalis biometrinių technologijų plėtros sąlygojamų problemų.

Problemų pagrindimas. Biometrinių duomenų netinkamas naudojimas iššaukia atitinkamas pasekmes, kurios gali būti itin pavojingos. Asmens duomenis, kaip ir privačią informaciją vis dažniau renka, saugo, bei perduoda daiktų interneto įrenginiai, naudojamos paslaugos debesyje, kas priveda prie galimų pažeidžiamumų asmens duomenims rizikų. Skirtingai nei tradicinės autentifikavimo sistemos, kaip slaptažodžiai, ar šifravimo raktai, biometrinės technologijos fiksuoja vieną unikalią tapatybę, kurios niekada negalima pakeisti. Dėl šio nekintančio biometrinių duomenų pobūdžio, šių

technologijų taikymas yra linkęs į sąlygojamas tapatybės grėsmes. Sukompromituoti biometriniai duomenys yra lengvas įsilaužėlių taikynys. Įgijus prieigą prie biometrinių duomenų, įsilaužėliai gali lengvai pavogti asmens tapatybę, ją pasinaudoti piktavališkais tikslais, ar sugadinti privačią informaciją, kuri gali turėti sunkius padarinius vartotojams naudojančioms šias technologijas. Saugumo problemos yra sutelkiamos į tai, kaip slapta informacija fiksuojama, saugoma, apdorojama, perduodama ir pasiekama. Biometrinius duomenis, kurie pasižymi nekintamumu, galima naudoti ir pasiekti įvairiais būdais, mažai dėmesio skiriant šių duomenų apsaugai, bei esant nepakankamam teisiniam reglamentavimui, tuo pačiu didėja ir sąlygojamos grėsmės. Šiuolaikiniai išmanieji įrenginiai, planšetiniai kompiuteriai ir fotoaparatai, ne tik fiksuoja kai kuriuos biometrinius duomenis, bet ir juos išsaugo, net jei jie nėra naudojami asmeniui autentifikuoti ar autorizuoti. Siekiant užkirsti kelią galimiems tapatybės vagystės atvejams, potencialioms grėsmėms duomenų apsaugai ir apsisaugoti nuo nesąžiningų veiksmų, reikalingas didesnis švietimas, bei informacijos sklaida. Reikalingas informacijos viešinimas, kaip yra apdorojami ir saugomi biometriniai duomenys, kokios yra galimos grėsmės naudojantis šiomis technologijomis. Reikalingas atidus biometrinių technologijų plėtros grėsmių vertinimas, kaip ir papildomų apsaugos priemonių taikymas, siekiant užtikrinti, kad vartotojų duomenys būtų saugūs, bei apsaugoti.

Darbo problema. Šiuo metu vis daugiau įmonių ir organizacijų pasitelkia biometrines technologijas kaip vieną iš galimų priemonių užtikrinti didesnę asmens duomenų saugumą ir patikimumą, lyginant su esamomis tradicinėmis autentifikacijos priemonėmis. Vykstanti nuolatinė biometrikos technologijų plėtra, įtakoja papildomas grėsmes ir rizikas asmens duomenų privatumui. Todėl yra svarbu suprasti kaip šios rizikos ir grėsmės įtakoja biometrinių duomenų vagystės ar neteisėtų asmens duomenų pasisavinimą, naudojimą. Svarbu pasitelkiant šių technologijų naudojimą, taikyti atitinkamą teisinį reglamentavimą ir švietimo sklaidą apie teikiamas naudas, bei rizikas. Kurti ir taikyti tinkamas apsaugos priemones, kurios padėtų apsaugoti asmens duomenis nuo neigiamų pasekmių.

Darbo objektas – biometrinių technologijų taikymas asmens tapatybei nustatyti, plėtros įtakojamos grėsmės asmens duomenų apsaugai.

Darbo tikslas – išanalizuoti biometrinių technologijų plėtros grėsmes asmens duomenų apsaugai.

Darbo uždaviniai:

1. Išnagrinėti biometrinių technologijų sampratą ir koncepciją.
2. Išanalizuoti biometrinių technologijų sąlygojamas grėsmes.
3. Ištirti Lietuvos vartotojų požiūrį į biometrines technologijas ir asmens duomenų saugumą.
4. Sukurti biometrinių technologijų plėtros Lietuvoje atsparumo grėsmėms modelį.

5. Pateikti rekomendacijas, kaip užtikrinti biometrinių technologijų plėtros atsparumą grėsmėms asmens duomenų apsaugai, atsižvelgiant į tyrimo rezultatus.

Darbo metodai:

1. Mokslinės literatūros analizė ir sisteminimas.
2. Tyrimų apžvalga ir analizė.
3. Kokybinė ir kiekybinė duomenų analizė.

Darbo struktūra:

Magistrinio darbo struktūra susideda iš penkių skyrių. Pirmame skyriuje pateikiamas darbo įvadas, kuriame apibūdinamas darbo aktualumas ir teorinis reikšmingumas, probleminis pagrindimas, darbo objektas, tikslas, uždaviniai ir metodai. Antroje dalyje nagrinėjami biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai, teoriniai aspektai. Trečias skyrius apima tyrimo metodologiją, naudojant kokybinę ir kiekybinę strategijas. Skyriuje pateikiamas tyrimo tikslas, keliama uždaviniai, taikomi metodai ir tyrimo eiga. Ketvirtame skyriuje pateikiami Lietuvos vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą empirinio tyrimo rezultatai. Skyriuje pateikiama ekspertų išsakyta nuomonė, rekomendacijos ir požiūris į biometrinės technologijas. Taip pat skyriuje pateikiamas Lietuvos vartotojų požiūris ir nuomonės šių technologijų naudojimo klausimu. Penktasis skyrius susideda iš išvadų ir rekomendacijų.

1. BIOMETRINIŲ TECHNOLOGIJŲ PLĖTROS GRĖSMĖS TEORINIAI ASPEKTAI

Šiame skyriuje aptariamos biometrinių technologijų plėtros grėsmės ir teoriniai aspektai. Pradžioje pateikiama biometrinių technologijų samprata ir koncepcija. Paaškinamos ir palyginamos autentifikavimo metodikos. Toliau skyriuje nagrinėjamas biometrinių technologijų veikimo principas, kuris yra grindžiamas biometrinių duomenų rinkimu ir analize, taip pat pateikiamos naujausios biometrikos plėtros tendencijos. Skyriuje analizuojamos biometrinių technologijų sąlygojamos grėsmės, kurios apima tokias grėsmių sritis kaip, atakos biometrinėse sistemose ir grėsmės privatumą išsaugančioms biometrinėms autentifikavimo sistemoms. Taip pat aptariamas asmens duomenų apsaugos reglamentavimo taikymas ir biometrikos, bei kibernetinio saugumo standartai, kurie yra būtini siekiant užtikrinti biometrinių technologijų saugumą ir efektyvumą.

1.1. Biometrinių technologijų samprata ir koncepcija

Biometrija – tai automatinis asmenų atpažinimas pagal jų fizinius ir elgsenos bruožus, naudojamas kaip metodas žinomų, ar nežinomų asmenų tapatybei nustatyti, taip suteikiant arba atimant galimybę naudotis tam tikromis privilegijomis ar teisėmis. Šis atpažinimo procesas grindžiamas prielaida, kad asmenys turi unikalių fizinių ir elgesio požymių, kurie juos išskiria iš kitų asmenų National Research Council. (2010). Pagal ISO/IEC 2382:2015 standartą biometriniai duomenys apibrėžiami kaip identifikavimo metodas, skirtas asmens tapatybei atpažinti ir patikrinti naudojant unikalios biologinius arba elgesio požymius. Pasitelkiant biometrines technologijas yra atliekami atitinkami matavimai, kurių rezultatai yra lyginami su patvirtintais duomenų bazėse saugomais pavyzdžiais, siekiant nustatyti sutaptį su anksčiau surinktais, saugomais skaitmeniniais asmens duomenimis (Anderson R, 2020).

Biometrinių technologijų koncepcija – grindžiama prielaida, kad kiekvienas žmogus turi savitų fiziologinių ar elgesio bruožų, išskiriančių jį iš kitų. Įvairūs autoriai teigia, kad biometriką galima apibrėžti kaip fiziologinių ir elgsenos požymių naudojimą siekiant atlikti asmens identifikaciją. Remiantis šiomis unikaliomis savybėmis, technologinę metodiką galima sugrupuoti į kelias kategorijas:

- **Fiziologiniai požymiai** – tai fizinės asmens savybės, kurias galima išmatuoti, pavyzdžiui, rankų geometrija, pirštų atspaudai, ar veido struktūra. Plaštakos geometrija apima asmens plaštakos dydžio ir formos matavimą, o pirštų atspaudai - unikalios pirštų galų briaunų ir raštų atspaudus. Veido atpažinimo technologijoje asmenims atpažinti naudojami veido taškai, pavyzdžiui, atstumas tarp akių ir žandikaulio linijos formos.

- **Elgsenos požymiai** – kurie apima asmens veiksmus, pavyzdžiui, parašą ir balsą, pagal kuriuos galima nustatyti asmens tapatybę. Parašai yra unikalūs, todėl tai, kaip asmuo pasirašo savo vardą ir pavardę, gali būti naudojami kaip biometrinis identifikatorius. Balso atpažinimo technologija naudoja asmens balso modelius jam identifikuoti ir yra plačiai naudojama saugumo ir stebėjimo sistemose.

Biometrinių duomenų taikymo tikslas – yra identifikuoti šios technologijos naudotoją, įvertinant atitinkamus biometrinius kriterijus, tokius kaip individualią asmens anatomiją, fiziologines savybes, įgūdžių spektrą, tam tikras elgesio savybes, ar šių kriterijų visumos aspektus (Anderson R, 2020). Surinkta informacija yra verčiama į analoginius arba skaitmeninius signalus, kurie tolimesniame etape naudojami duomenų apdorojimui. Šiuo būdu gauti duomenys gali būti naudojami žmonių tapatybei nustatyti. Svarbu paminėti ir tai, kad biometriniai duomenys kiekvienam asmeniui yra unikalūs ir gali būti pasitelkiami asmens tapatybei nustatyti, tiek civiliniame sektoriuje, kaip sveikatos priežiūros, švietimo įstaigos, įmonėse, taip pat ir kariuomenėje, policijoje, ar valstybės institucijose, siekiant apsaugoti tam tikrą informaciją, bei išteklius. Todėl biometrinio autentifikavimo informacinėse technologijose taikymas išskiriamas kaip, viena iš naudotojų identifikavimo ir prieigos prie saugomų išteklių kontrolės forma (Tota ir kt., 2019).

Atsižvelgiant į tai, kad biometrinės technologijos sudaro nemažai savitų asmens biologinių savybių, kurios išskiriamos kaip biometriniai duomenys, anot autoriaus Bolle (2006) atsiranda poreikis šias technologines savybes, kaip ir taikomas priemones išskirti pagal tam tikrus kriterijus. Kriterijai reikalingi siekiant įvertinti biometrinių technologijų patrauklumą, kaip ir galimas naudas su trūkumais, todėl technologijos yra skirstomos pagal šiuos pagrindinius reikalavimus:

- **Unikalumas** – šis požymis reiškia identifikavimo tikslais naudojamo biometrinio požymio ar savybės išskirtinumą. Biometriniai požymiai yra unikalūs ir laikui bėgant nekinta, todėl jie yra vienas iš patikimumą didinančių savybių asmens identifikavime. Šis unikalumo požymis grindžiamas tuo, kad nėra dviejų vienodų pirštų atspaudų, akies rainelės raštų ar veido bruožų. Elgesio požymiai, pavyzdžiui, parašas ir balsas, taip pat pasižymi unikalumais savybėmis, dėl kurių juos galima patikimai naudoti identifikavimo tikslais.

- **Pastovumas** – požymis nurodantis, kad biometriniai požymiai laikui bėgant išlieka santykinai nepakitę. Tai svarbi biometrinio požymio savybė, nes ji užtikrina, kad sistema gali tiksliai identifikuoti asmenį laikui bėgant, net jei jis sensta ar fiziškai keičiasi. Biometrinės sistemos įprastai kuriamos taip, kad būtų atsižvelgta į biometrinių požymių pastovumo požymį, naudojant algoritmus, kurie gali aptikti ir atsižvelgti į pokyčius laikui bėgant. Sistemos taip pat gali reikalauti, kad asmenys periodiškai atnaujintų savo biometrinius duomenis, siekiant užtikrinti, kad duomenys būtų tikslūs ir aktualūs.

- **Našumas** – savybė nusakanti duomenų pralaidumą, registravimo laiką ir tikrinimo laiką. Našumas apibūdinamas kaip asmenų, kuriuos sistema gali apdoroti per tam tikrą laikotarpį, skaičių,

registravimo laiką, kurio reikia naujam naudotojui užregistruoti ir tikrinimo laiką, kurio reikia asmens tapatybei patikrinti.

- **Apėjimas** – savybė reiškia asmens gebėjimą išvengti biometrinės sistemos autentiškumo nustatymo proceso. Tai gali įvykti naudojant alternatyvius autentifikavimo metodus, pavyzdžiui, pateikiant suklastotą biometrinių pavyzdžių arba naudojant pavogtą įgaliojimą. Apėjimo funkcija gali pakenkti biometrinių sistemų veiksmingumui, nes suteikia galimybę neleistinai patekti į neskelbtiną informaciją ar sritis.

- **Apdorojimo sparta** – požymis yra labai svarbus biometrinių technologijų našumo veiksnys, nes nuo jo priklauso, kaip greitai ir efektyviai sistema gali nustatyti naudotojų autentiškumą. Apdorojimo greitis reiškia laiką, per kurį sistema užfiksuoja ir apdoroja biometrinius duomenis, suderina juos su saugomais šablonais ir nustato naudotojo tapatybę. Didesnis apdorojimo greitis gali pagerinti naudotojų patirtį, padidinti pralaidumą ir padidinti saugumą, nes sumažėja nesankcionuotos prieigos rizika, dėl vėlavimo nustatant tapatybę.

- **Tikslumas** – požymis nusakantis biometrinių technologijų našumą, nuo kurio priklauso, koku tikslumu sistema gali patvirtinti naudotojų autentiškumą. Biometrinių sistemų tikslumas paprastai išreiškiamas klaidingo priėmimo dažnio (FAR) ir klaidingo atmetimo dažnio (FRR) rodikliais. FAR reiškia, kad sistema neteisingai nustato neįgaliojų naudotojų autentiškumą, o FRR reiškia, kad sistema nesugeba nustatyti įgaliojų naudotojų autentiškumo. Didelis tikslumas yra labai svarbus siekiant užtikrinti sistemos saugumą ir užkirsti kelią neteisėtai prieigai Jain, A. K., Ross, A., ir Nandakumar, K. (2016).

Išvardinti biometriniai požymiai dar gali būti skirstomi į minkštuosius ir kietuosius Chhabra, G., ir Narayanan, A. (2013). Minkštieji biometriniai požymiai yra linkę per tam tikrą laiką keistis, tai labiau būdinga balsui, rašysena ar eisenai. Kietieji biometriniai požymiai yra laikomi pastovios būsenos ir laiko prasme turintys mažą tikimybę keistis, pavyzdžiui akių rainelė, pirštų atspaudai ar delno atspaudas.

Siekiant įvertinti ir klasifikuoti skirtingų biometrinių metodų taikymo efektyvumą, bei patikimumą galima remtis apžvelgtomis, šešiomis pagrindinėmis savybėmis (žr. 1 lent.).

1 lentelė. Įvairių biometrinių metodų palyginimas pagal savybes

Biometrinės priemonės	Unikalumas	Pastovumas	Našumas	Apėjimas	Apdorojimo sparta	Tikslumas
Pirštų atspaudai	Aukštas	Vidutinis	Vidutinis	Vidutinis	Aukšta	Vidutinis
Venų raštas	Vidutinis	Vidutinis	Vidutinis	Žemas	Vidutinė	Vidutinis
Rankų geometrija	Vidutinis	Žemas	Vidutinis	Vidutinis	Aukšta	Vidutinis
Balsas	Aukštas	Žemas	Vidutinis	Aukštas	Aukšta	Žemas
Rainelė	Aukštas	Aukštas	Aukštas	Žemas	Vidutinė	Aukštas
Tinklainė	Aukštas	Aukštas	Aukštas	Žemas	Vidutinė	Aukštas
Veidas	Vidutinis	Vidutinis	Žemas	Aukštas	Vidutinė	Žemas
Klavišų paspaudimas	Žemas	Žemas	Žemas	Vidutinis	Vidutinė	Žemas
Parašas	Aukštas	Žemas	Vidutinis	Aukštas	Aukšta	Vidutinis

Šaltinis: adaptuotas pagal Gupta, P. ir Gupta, P., 2017

Remiantis informacija pateikiama 1 lentelėje, lyginant skirtingų biometrinių duomenų rinkimo metodikas, galima išskirti saugesnes, tikslesnes ir didesniu patogumu pasižyminčias technologijas. Žvelgiant iš saugumo pusės, pirštų atspaudų, venų raštų, rainelės ir tinklainės biometriniai duomenys yra laikomi saugesne alternatyva, užtikrinančia pakankamą arba aukštą unikalumo lygį, sunkų atkartojimą, suklastojimą. Rankos geometrija, veido, balso, klavišų paspaudimo ir parašo biometrija galima laikyti mažiau saugia, nes ją galima atkartoti arba tam tikru mastu imituoti. Akcentuojant tikslumą, dėl didelio unikalumo ir stabilumo laikui bėgant akies rainelės, tinklainės ir pirštų atspaudų biometrija yra tiksliausia. Rankos geometrija, venų raštas, veidas ir balsas laikomi vidutiniškai tiksliais biometriniais duomenimis, tačiau jiems gali turėti įtakos anksčiau paminėti išvaizdos pokyčiai, senėjimas ar fiziniai pažeidimai. Klavišų paspaudimo ir parašo biometrija yra mažiau tiksli, dėl spausdinimo ar pasirašymo elgsenos svyravimų. Naudojimo patogumo prasme rankos geometrija, veido, balso, klavišų paspaudimo ir parašo biometriniai duomenys galima laikyti patogesniais naudoti, nes jiems nereikia fizinio kontakto su jutikliu ar specialios įrangos ir juos galima lengvai integruoti į kasdienę veiklą. Pirštų atspaudų, venų raštų, akies rainelės ir tinklainės biometriniai duomenys gali būti mažiau patogūs naudoti, nes jiems reikia fizinio kontakto su jutikliu, arba jie gali būti labiau invazinio tipo.

Apibendrinant 1 lentelėje pateikiamas išvadas matyti, kad tiksliausios biometrinės technologijos vis tik yra pirštų atspaudai ir akies rainelė / tinklainė. Tačiau technologijos pasirinkimas visada priklausys nuo konkretaus naudojimo atvejo, kompromisų tarp saugumo, tikslumo ir patogumo.

1.2. Biometrinės technologijos ir jų veikimo principas

Vykstant sparčiai informacinių technologijų plėtrai, palaipsniui didėja sistemų ir kompiuterių informacijos apdorojimo sparta, auga išmanių įrenginių, bei taikomųjų programų įvairovė. Todėl atsiranda poreikis kurti ir taikyti efektyvesnes, tam tikrais atvejais patogesnes kasdieniam naudojimui saugumo technologijas, kurios užtikrintų didesnę saugumo lygį, lyginant su jau įprastu slaptažodžių taikymo principu grįstomis autentifikavimo sistemomis. Vis dažniau taikant autentifikavimo sistemų sprendimus yra pasitelkiamos ir biometriniais duomenimis grįstos identifikavimo technologijos, kurios palaipsniui vykstant technologijų plėtrai tampa svarių pagrindų technologijų taikymo srityje.

Analizuojant naudojamas biometrines technologijas ir jų duomenų naudojimą pasauliniu mastu, labiausiai iš visų biometrikoje išskiriamų sąvokų yra atpažinimas. Biometrinių duomenų taikymo procese, atpažinimo sąvoka suprantama, kaip procesas kurio metu biometrinė sistema bando atpažinti atitinkamą asmenį, atliekant tapatybės nustatymo sutaptį su išsaugotais, turimais įrašais. Šiuo principu yra grindžiamos visos šiuo metu naudojamos biometrinės technologijos, priklausomai nuo pasirinkto techninio sprendimo, skiriasi tik atpažinimo taikymo metodika. Atpažinimo tikrinimas veikia duomenų tarpusavio sutapties palyginimo principu ir apima biometrinių duomenų palyginimą vienas su kitu, ko

pasėkoje esant sutapčiai suteikiama prieiga prie naudojamos paslaugos, objekto ar skaitmeninio turinio (pvz., išmaniojo įrenginio, taikomosios programinės įrangos, kompiuterių tinklo ar duomenų bazės) (Tota ir kt., 2019). Palaipsniui biometrinių duomenų naudojimas įsisavinamas kaip papildoma priemonė ar net pakaitalas tradiciniams autentifikacijos būdams (pvz. slaptažodžiai ar PIN kodai), taip siekiant supaprastinti ir palengvinti prieigos kontrolę. Lyginant gyvą asmens biometrinį mėginį su vienu patikimu saugomu pavyzdžiu, nustatoma asmens tapatybė (Lalović ir kt., 2015). Pavyzdys gali būti saugomas centrinėje duomenų bazėje, išmaniajame įrenginyje, arba laikomas prieigos raktu, pvz. asmens tapatybės kortelė (Lalović ir kt., 2016a).

Šiuo metu galima išskirti per dešimt naudojamų atpažinimo principu grįstų, biometrinio identifikavimo metodikų, pasižyminčių specifiniais veikimo principais ir savybėmis:

Pirštų atspaudų atpažinimas – tai technologija, naudojanti unikalias fizines asmens pirštų atspaudų savybes, tapatybės nustatymui ir patvirtinimui. Pirštų atspaudų atpažinimo galimybė šiuo metu naudojama daugelyje programų, įskaitant išmanių įrenginių prieigos autentifikavimą, užtikrinant fizinę prieigos kontrolę, privačiuose ir viešuosiuose sektoriuose.

Šalyse, kuriose yra didelis neraštingumo lygis, bankai naudoja pirštų atspaudus klientams identifikuoti. Kaip pavyzdį galima išskirti Indiją, kurioje nacionaliniu mastu buvo sukurta ir pradėta taikyti „Aadhaar“ sistema, su tikslu saugoti sistemos naudotojų pirštų atspaudus ir akies rainelės koduotą informaciją. Pačioje sistemos taikymo pradžioje buvo orientuojamasi į socialines išmokas, tačiau palaipsniui didinant galimybes, pereita prie banko sąskaitų atidarymo, taip pat išmaniųjų telefonų registracijos, paskutiniame etape įdiegti sprendimai palengvinantys tokių funkcijų taikymą teisėsaugos klausimų ar teismo ekspertizių vykdyme (Singh S, 2018).

Žvelgiant į pirštų atspaudų autentifikavimo pranašumus galima išskirti tai, kad dauguma žmonių jau yra susipažinę su šia technologija, ar net reguliariai naudojami įrenginiais, kur šie sprendimai yra pritaikyti. Pats technologinis sprendimas yra pakankamai ekonomišką, paprastas pritaikyti įvairiose informacinėse sistemose ir įrenginiuose. Tačiau technologijų dispersija gali būti ir trūkumas, nes pigesnėse sistemose didėja klaidingų atpažinimų ir klaidingai patvirtintų teigiamų rezultatų rodiklis. Klaidų tikimybių atsiradimas yra įtakojamas įvairių veiksnių, tokių kaip amžiaus skirtumas, turimi apsigimimai, traumos ar kitokio pobūdžio atsiradę paviršiaus pakeitimai, bei pažeidimai.

Pirštų atspaudų identifikavimo sistemos taip pat turi tam tikras sąlygojančias grėsmes, tokias kaip įvairių atakų riziką, įgyvendinamą elektroninėmis priemonėmis, taip pat fizinių savybių manipuliavimo atvejus, kuomet sistema įtakojama papildomais veiksmais pirštų nuskaitymo etape pakeičiant eiliškumą ar nuskaitymų pirštų tvarką. Tačiau susirūpinimą kelia ir biometrinių duomenų privatumas ir saugumas. Kaip pažymėjo Ross, Nandakumar ir Jain (2017), biometriniai duomenys yra labai jautrūs ir gali būti naudojami kenkėjiškiems tikslams, jei jie patenka į netinkamas rankas. Nepaisant įvairių potencialių grėsmių ir apribojimų, pirštų atspaudų identifikavimo sistemos taikymas

gali atgrasyti nuo sukčiavimo asmens tapatybe (Anderson R, 2020). Remiantis Jain, Ross ir Nandakumar (2016) atliktu tyrimu, pirštų atspaudų atpažinimo tikslumas yra didesnis, lyginant su kitomis technologijomis, tokiomis kaip veido ar rainelės atpažinimo. Tyrimas parodė, kad pirštų atspaudų atpažinimo klaidingo atmetimo procentas buvo tik 0,1%, o klaidingo priėmimo procentas buvo vos 0,00001%. Taip atliktų tyrimų metu įrodyta, kad pirštų atspaudų atpažinimo technologijos naudojimas pagerina įvairių sistemų saugumą ir patogumą. Pavyzdžiui, Bond, Hassouna ir Buford (2015) tyrime nustatyta, kad pirštų atspaudų atpažinimo technologijos įdiegimas išmaniajame telefone padidina vartotojų pasitenkinimą ir sumažina bandymų įvesti neteisingą slaptažodį skaičių.

Venų rašto atpažinimas – tai biometrinė technologija, kurioje asmens tapatybei nustatyti ir autentiškumui patvirtinti naudojamas unikalus asmens kūno venų raštas, esantis pirštuose arba plaštakos nugarėlėje. Ši technologija buvo sukurta kaip alternatyva tradiciniams biometriniais metodams, tokiems kaip pirštų atspaudų atpažinimas ir akies rainelės atpažinimas, siekiant užtikrinti didesnę tikslumą ir saugumą. Remiantis Ross ir Jain (2015) atliktu tyrimu, venų raštų atpažinimo technologija turi keletą privalumų, palyginti su kitomis biometrinėmis technologijomis. Pavyzdžiui, ją mažiau veikia išoriniai veiksniai, tokie kaip odos būklės pokyčiai, senėjimo įtakojami pakitimai, ar atsiradę sužeidimai, būtent tai didina šio biometrinio metodo taikymo patikimumą ilgalaikio indentifikavimo perspektyvoje. Be to, laikoma, kad venų raštai yra unikalesni ir sunkiau dubliuojami, palyginti su kitais esančiais biometriniais metodais, todėl suteikia papildomą saugumo lygį. Pavyzdžiui, Bhardwaj et al. (2020 m.) atliktame tyrime buvo nagrinėjamas venų raštų atpažinimo naudojimas biometrinėse programose, finansinių operacijų atlikimo apsaugai padidinti. Tyrėjai sukūrė sistemą, kuri, naudodama artimosios infraraudonosios spinduliuotės vaizdus, užfiksavo asmens rankos venų raštus, o tolimesniame etape naudojo mašininio mokymosi algoritmus šiems raštams analizuoti ir nustatyti jų autentiškumą. Sistema parodė didelį tikslumą, dėl ko prieita prie išvados, kad kaip alternatyvus metodas galėtų būti naudojama finansų įstaigose, siekiant užkirsti kelią sukčiavimo galimybėms, tuo pačiu taip padidinant saugumą. Žvelgiant į venų raštų atpažinimo pritaikymą ir panaudojimą autentifikavimui mobiliuosiuose įrenginiuose, Fang et al. atliktame tyrime (2019 m.) buvo sukurta sistema, kuri naudojo išmaniojo telefono kamerą ir artimųjų infraraudonųjų spindulių šviesą, kad užfiksuotų ir išanalizuotų asmens piršto venų raštus. Ši sukurta sistema taip pat pademonstravo didelį tikslumą taikant venų atpažinimo metodiką, taip pat atskleidė potencialias pritaikymo galimybes saugaus autentifikavimo mobiliuosiuose įrenginiuose užtikrinimui.

Rankų geometrijos atpažinimas – technologija, kuri naudoja asmens plaštakos fizines savybes, tokias kaip, dydis, forma ir ilgis, kad nustatytų ir patvirtintų jo tapatybę. Ši technologija plačiai naudojama įvairiose srityse, įskaitant prieigos kontrolės sistemas, darbo laiko apskaitos sistemas ir kriminalinius tyrimus. Remiantis Jain, Ross ir Nandakumar (2016) atliktu tyrimu, rankos geometrijos atpažinimo technologija, palyginti su kitomis biometrinėmis technologijomis, pasižymi sąlyginai

nemažu tikslumu, bei mažais klaidingų atmetimo, ar klaidingų priėmimo autentifikacijų atvejais. Tyrime nustatyta, kad rankos geometrijos atpažinimo technologija yra ypač veiksminga didelės apimties identifikavimo sistemose, kuriose reikia greitai ir tiksliai apdoroti didelį skaičių asmenų. Taip pat paaiškėjo, kad rankos geometrijos atpažinimo technologijos naudojimas yra ekonomiškai efektyvus. Pavyzdžiui, Ross ir Jain (2015) atlikto tyrimo metu nustatyta, kad didelėje įmonėje įdiegus plaštakos geometrijos atpažinimo technologiją sumažėjo laiko ir išlaidų, susijusių su rankiniu darbo laiko apskaitos procesu.

Tačiau yra ir tam tikrų apribojimų, susijusių su rankų geometrijos atpažinimo technologija. Pavyzdžiui, asmens rankos formos pokyčiai, kaip traumos, ar svorio kritimas, gali turėti svarios įtakos technologijos tikslumui ir patikimumui. Be to, kai kurie asmenys gali turėti unikalią rankos formą, kurią gali būti sunku tiksliai išmatuoti, dėl ko klaidingų atmetimų atvejų skaičius išaugtų.

Balso atpažinimas – balso atpažinimas analizuoją asmens balsą, kad patikrintų jo tapatybę. Kvėpavimo takai ir minkštųjų audinių ertmės, taip pat burnos ir žandikaulio forma ir judėjimas įtakoja balso modelius, sukuriant unikalų balso atspaudą Aware. (2020). Balso atpažinimo funkcija pirmiausia naudojama laisvų rankų įrangos mobiliam autentifikavimui, saugaus vairavimo alternatyvai, tais atvejais kai veido atpažinimas, pirštų atspaudų atpažinimas ir kitos biometrinės autentifikavimo formos yra nesaugios. Pasak autoriaus Anderson, R. (2020), balso atpažinimo technologija naudojasi vyriausybės tarnybos ir privačios organizacijos. Pavyzdžiui teismo fonologijoje, naudojamoje kriminaliniams tyrimams, įrašytas balsas lyginamas su visų perspektyvių įtariamųjų kalbos pavyzdžiais. Žvelgiant į tyrimus atliktus technologijos taikymo kontekste, Chen ir kt. (2020) tyrime buvo nagrinėjamas balso biometrijos naudojimas saugiam autentifikavimui mobiliuosiuose įrenginiuose. Tyrimo metu buvo sukurta sistema naudojanti mašininio mokymosi algoritmus, kuri analizavo unikalios asmens balso ypatybes, tokias kaip balso aukštumą ir tembrą, siekiant atlikti autentifikaciją patvirtinant tapatybę. Sistema pasižymėjo dideliu tikslumu ir palankiomis galimybėmis naudojimui ir pritaikymui mobiliuosiuose įrenginiuose. Kitame tyrime, kurį atliko Islam ir kt. (2021), buvo nagrinėjamas balso atpažinimo panaudojimas gilių netikrų garso įrašų atakoms aptikti ir galimybėms užkirsti joms kelią. Tyrėjai sukūrė sistemą, kuri taikydama mašininio mokymosi algoritmus, analizavo unikalios asmens balso modelius ir aptiko bet kokias anomalijas ar neatitikimus, galinčius rodyti giluminį suklastotą garso įrašą. Tyrimo metu sukurta sistema demonstravo didelį tikslumą ir puikias pritaikymo galimybes naudojimui taikomose programose, siekiant galimų sukčiavimo atvejų nustatymui. Apibendrinant tyrimų rezultatus, galima išskirti tam tikrus privalumus ir trūkumus. Pagrindinis technologijos privalumas yra tas, kad autentifikavimo galimybė gali būti taikoma ir prieinama visuose skaitmeniniuose įrenginiuose turinčiuose mikrofonus, taip pat įvairių funkcijų valdymas balsu yra patogus naudotojų atžvilgiu. Pati technologija yra pažystama ir ekonomiškai efektyvi. Trūkumų išskiriama kiek daugiau, pavyzdžiui balso atpažinimas nėra

pasižymintis tokiu tikslumu, kaip kai kitos apžvelgtos biometrinės technologijos. Taip pat reikalauja gyvumo nustatymo, siekiant patikrinti autentiškumą, yra stipriai įtakojamas išorinių veiksnių, tokių kaip foninis triukšmas, kas turi įtakos tiksliai įrašo atlikimui ir sutapties patikrai.

Rainelės atpažinimas – rainelės atpažinimas yra biometrinė technologija, kuri naudoja unikalios asmens akies rainelės raštus, kad nustatytų ir patvirtintų jo tapatybę. Rainelė, akies raumuo, reguliuojantis vyzdžio dydį, turi kiekvienam individui būdingus raštus. Dėl to dešimtajame dešimtmetyje tapatybės patvirtinimui buvo sukurta rainelės atpažinimo technologija Aware. (2020). Rainelės atpažinimo technologija laikoma labai tiksli ir patikima dėl unikalios rainelės raštų, kurie laikui bėgant išlieka stabilūs ir yra sunkiai pamėgdžiojami (Ross, Nandakumar ir Jain, 2021). Rainelė taip pat turi daugiau unikalios savybių nei kitos biometrinės technologijos, pavyzdžiui, pirštų atspaudai, kurie padeda padidinti atpažinimo proceso tikslumą (Jain ir Ross, 2020). Nuo 2005 metų, kai nustojo galioti pirminiai patentai, dėka akies rainelės atpažinimo technologijos greičio ir tikslumo, ji tapo komerciškai prieinamesnė biometrinio identifikavimo forma. Rainelės atpažinimo technologija veikia fiksuodama spalvotą akies dalį, esančią aplink vyzdį. Po to šis vaizdas yra apdorojamas, kad būtų išgaunamos tam tikros unikalios savybės, tokios kaip rainelės kreivumas ir tekstūra, vėliau šios savybės yra naudojamos kuriant skaitmeninį rainelės šabloną (Jain ir Ross, 2020). Šis šablonas naudojamas kaip nuoroda palyginimui su būsimais rainelės vaizdais, siekiant patvirtinti asmens tapatybę. Rainelės atpažinimo procesą paprastai sudaro trys etapai, rainelės lokalizacija, savybių ištraukimas ir suderinimas (Ross, Nandakumar ir Jain, 2021). Rainelės lokalizacijos metu rainelė yra segmentuojama iš aplinkinių audinių ir kitų akies dalių. Naujai užfiksuotas rainelės vaizdas yra lyginamas su atskaitos šablonu, taip siekiant patvirtinti asmens tapatybę.

Naujausi tyrimai parodė, kad rainelės atpažinimo technologija yra labai tiksli ir patikima biometrinė technologija. Ross, Nandakumar ir Jain (2021) atliktas tyrimas parodė, kad rainelės atpažinimo technologija pasižymi mažu klaidingų atmetimų, bei klaidingo priėmimo dažniu, taip pat pasižymi aukštu efektyvumu identifikavimo sistemose, kur reikalingas greitas ir tikslus asmenų indentifikavimas.

Tinklainės atpažinimas – biometrinė technologija, kurioje siekiant nustatyti asmens tapatybę naudojamos akies vidinėje dalyje esančios kraujagyslės, kurios pasižymi unikaliosiomis savybėmis. Atpažinimo procesas vykdomas fiksuojant didelės raiškos tinklainės vaizdą ir jį apdorojant, tam pasitelkiant specialiai pritaikytas kameras, skirtas apšviesti akies vidinę dalį pasitelkiant infraraudonąją šviesą. Tada vaizdas yra apdorojamas naudojant algoritmus, kurie nustato ir analizuoja unikalų tinklainės kraujagyslių raštą. Išgautas raštas yra palyginamas su jau egzistuojančia raštų duomenų baze, kad būtų galima nustatyti asmens autentiškumą (Mauro, 2022). Tinklainės atpažinimo procesas paprastai apima tris etapus: tinklainės lokalizaciją, funkcinių savybių ištraukimą ir suderinamumą. Tinklainės lokalizacijos metu tinklainė yra segmentuojama iš aplinkinių audinių ir kitų akies dalių.

Tinklainės atpažinimo technologija yra laikoma viena tiksliausių ir patikimiausių biometrinių technologijų, dėl unikalių tinklainės raštų, kurie laikui bėgant yra stabilūs ir sunkiai pamėgdžiojami (Jain ir Ross, 2020). Tinklainėje taip pat yra daug unikalių savybių, kurios padeda padidinti atpažinimo proceso tikslumą (Ross, Nandakumar ir Jain, 2021). Būtent, dėl šių savybių, atliktuose moksliniuose tyrimuose akies tinklainės technologija išskiriama, kaip pasižyminti didžiausiu stabilumu. Skirtingai nei kiti biometrinių autentifikavimo būdai, pavyzdžiui, pirštų atspaudų atpažinimo technologija, tinklainės atpažinimo procesui įtakos neturi išoriniai veiksniai, tokie kaip nešvarumai ar odos įpjovimai (Mauro, 2022).

Nepaisant didelio tikslumo, tinklainės atpažinimo technologija turi ir tam tikrų apribojimų. Vienas iš pagrindinių iššūkių, reikalingos specializuotos kameros su papildoma įranga, kas yra pakankamai brangu ir sunkiau prieinama, lyginant kitų technologijų panaudojimą. Taip pat anot autoriaus Mauro (2022) nustatyta, jog tinklainės atvaizdo fiksavimo procesas kai kuriems asmenims gali būti nepatogus, todėl gali sumažėti teisingai identifikuotų naudotojų atvejų kiekis.

Veido atpažinimas – biometrinė technologija naudojanti unikalius asmens veido bruožus, siekiant patvirtinti tapatybę. Veido atpažinimo procesas veikia fiksuojant asmens veido vaizdą ir jį apdorojant, kad būtų išgaunami unikalūs bruožai, pvz., akių, nosies, burnos forma ir kitos savybės. Tada ši informacija naudojama kuriant skaitmeninį šabloną, kuris naudojamas kaip nuoroda palyginimui su būsimais veido vaizdais, siekiant patvirtinti asmens tapatybę. Veido atpažinimo procesas paprastai apima tris etapus: veido aptikimą, funkcijų ištraukimą ir suderinimą. Veido aptikimo metu programinė įranga aptinka veidą vaizde. Funkcijų ištraukimo metu išgaunami unikalūs veido bruožai kurie po to naudojami šablono sukūrimui. Galiausiai derinimo etape, naujai užfiksuotas veido vaizdas lyginamas su atskaitos šablonu, siekiant patvirtinti asmens tapatybę. Veido atpažinimo technologija pastaraisiais metais labai patobulėjo dėl mašininio mokymosi progreso ir kompiuterinio matymo pažangos. Pasak autorių Jain ir Ross, (2020) ši technologija naudojama įvairiose sistemose ir programose, tokiose kaip sienų kontrolė, teisėsaugos institucijose ir prieigos kontrolės sistemose. Tačiau veido atpažinimo technologija nėra be apribojimų, todėl vyksta diskusijos dėl jos tikslumo, privatumo pasekmių ir etinių problemų (Ross, Nandakumar ir Jain, 2021).

Veido atpažinimo technologija turi ir tam tikrų pranašumų, kaip ir iššūkių, lyginant su kitomis. Kaip pranašumą galima išskirti tai, jog yra daug skaitmeninių veido vaizdo duomenų, kuriuos galima laisvai pasiekti ir atsisiųsti internete. Surinkus didesnius kiekius viešai internete prieinamų pavyzdžių, naudojamus algoritmus galima išmokyti veikti tinkamai, pasitelkiant mašininio mokymosi metodus Aware. (2020). Taip pat, dėl plataus išmaniųjų įrenginių ir kompiuterių su įmontuotomis kameromis naudojimo, tampa patogų rinkti gyvus pavyzdžius. Vaizdo atpažinimas taip pat gali būti atliekamas tuo pačiu metu kaip ir kiti tikrinimo procesai, pvz., balso atpažinimas, pirštų atspaudų nuskaitymas ar klavišų paspaudimų modelių nustatymas Aware. (2020). Iššūkiai su kuriais susiduria veido atpažinimo

technologija, dažnai siejasi su apšvietimo poveikiu, senėjimu ir akinių ar veido plaukų buvimu, įskaitant etninio šališkumo argumentus. Fotonuotraukų darymas taip pat gali sukelti prieštaringų atitikimo rezultatų. Vienas didžiausių veido atpažinimo technologijos iššūkių yra didelis vaizdų, pasiekiamų internete per socialinę žiniasklaidą ir kitus svetainių profilius skaičius, kuris iš vienos pusės palengvina mašininių mokymąsi, iš kitos atveria esamų spragų išnaudojimo galimybes.

Klavišų paspaudimų atpažinimas – yra biometrinė technologija, kuri naudoja unikalų asmens rašymo ritmą ir modelį, kad patvirtintų jo tapatybę, dar suprantama kaip klavišo paspaudimų dinamika. Klavišų paspaudimų atpažinimo procesas veikimo principas susideda iš laiko tarp klavišų paspaudimų ir klavišų paspaudimų trukmės įvedant konkrečią simbolių seką analizės. Ši informacija naudojama kuriant skaitmeninį šabloną, kuris naudojamas kaip nuoroda palyginimui su būsimais klavišų paspaudimų modeliais, siekiant patvirtinti asmens tapatybę. Klavišų paspaudimų atpažinimo procesas susideda iš duomenų surinkimo, funkcijų ištraukimo ir suderinimo. Renkant duomenis, klavišų paspaudimų modeliai yra registruojami ir analizuojami. Funkcijų išskleidimo metu unikalios klavišų paspaudimo modelio savybės išgaunamos ir naudojamos šablonui sukurti. Galiausiai naujai įrašytas klavišo paspaudimo modelis derinamas ir lyginamas su atskaitos šablonu, siekiant patvirtinti asmens tapatybę.

Klavišų paspaudimų atpažinimo technologija plačiai naudojama įvairiose programose, tokiose kaip saugios prisijungimo sistemos, internetinė bankininkystė ir saugi prieiga prie jautrios informacijos (Jain & Ross, 2020). Ši technologija laikoma saugia ir patikima, nes sunku imituoti asmens klavišų paspaudimų modelį, o klavišų paspaudimų atpažinimo procesą galima derinti su kitomis biometrinio autentifikavimo formomis, taip siekiant padidinti saugumą (Ross, Nandakumar ir Jain, 2021).

Parašo atpažinimas – yra biometrinė technologija, kuri naudoja unikalų asmens parašą, kad patvirtintų jo tapatybę. Parašo atpažinimo procesas vyksta fiksuojant suskaitmenintą asmens parašo vaizdą ir jį apdorojant, kad būtų išskirtos unikalios savybės, pvz., parašo forma, greitis ir spaudimas. Remiantis šiomis savybėmis ir surinkta informacija, kuriamas skaitmeninis šablonas, kuris naudojamas kaip nuoroda palyginimui su būsimais parašais, siekiant patvirtinti asmens tapatybę. Parašo atpažinimo procesas kaip ir įprastai atpažinimo technologijose apima tris etapus: išankstinį apdorojimą, funkcijų ištraukimą ir suderinimą. Išankstinio apdorojimo metu parašo vaizdas konvertuojamas į skaitmeninį formatą ir pašalinamas triukšmas. Išskleidus ypatybes, išskirtinės parašo savybės išgaunamos ir naudojamos šablonui sukurti. Galiausiai derinant naujai užfiksuotas parašo vaizdas lyginamas su nuorodos šablonu, siekiant patvirtinti asmens tapatybę.

Parašo atpažinimo technologija plačiai naudojama įvairiose programose, tokiose kaip saugios prisijungimo sistemos, internetinė bankininkystė ir saugi prieiga prie jautrios informacijos (Jain & Ross, 2020). Ši technologija laikoma saugia ir patikima, nes sunku imituoti asmens parašą, o parašo

atpažinimo procesą taip pat galima derinti su kitomis biometrinio autentifikavimo formomis, siekiant padidinti saugumo lygį (Ross, Nandakumar ir Jain, 2021).

Žmogaus lusto implantavimo technologija – žmogaus mikroschemos implantavimas, dar vadinamas žmogaus mikroschemų įsodinimu, tai mažos mikroschemos įterpimas į žmogaus kūną identifikavimo ir sekimo tikslais. Mikroschemoje gali būti saugoma asmeninė informacija, pvz., medicininė istorija, kontaktinė informacija ir identifikavimo duomenys. Biometrijos srityje žmogaus lusto implantavimas tiriamas kaip priemonė asmens saugumui didinti ir tapatybei tikrinti.

Žmogaus lusto implantavimo šalininkai teigia, kad tai gali padėti sumažinti tapatybės klastojimo ir vagysčių atvejų skaičių, taip pat pagerinti reagavimo į skubios medicinos pagalbos atvejus laiką. Tačiau kritikai išreiškė susirūpinimą dėl privatumo, saugumo ir galimybės piktnaudžiauti asmens duomenimis. Keliuose tyrimuose nagrinėtos žmogaus lusto implantavimo biometrikoje galimybės ir reikšmė. Pavyzdžiui, 2019 m. Ghatak ir Ray apžvalginiam straipsnyje nagrinėjo įvairias žmogaus lusto implantavimo taikymo sritis, įskaitant sveikatos priežiūrą, saugumą ir prieinamumą. Autoriai taip pat aptarė su šia technologija susijusius etinius ir teisinius aspektus, pažymėdami, kad reikia patikimų duomenų apsaugos priemonių ir informuoto sutikimo protokolų taikymo. Kitame tyrime, kurį atliko Gao ir kt. (2019), buvo nagrinėjamas radijo dažnių atpažinimo (RFID) technologijos naudojimas žmonių identifikavimui ir sekimui. Tyrėjai sukūrė RFID lustų implantavimo į peles sistemą ir pademonstravo, kad ją galima naudoti biometrinėse programose, pavyzdžiui, prieigos kontrolei ir autentiškumo nustatymui. Apskritai, nors žmogaus lustų implantavimo panaudojimas biometrikoje tebėra kontraversiška tema, vykdomi tyrimai rodo, kad jis gali suteikti daugybę privalumų ir taikymo galimybių. Kai kurios didelės tarptautinės įmonės dar tik diskutuoja galimus scenarijus, siekdamos įtraukti savo darbuotojus į mikroschemų naudojimą, žmogaus teisių ir privatumo grupės yra susirūpinusios, kad netolimoje ateityje darbuotojai gali būti verčiami naudotis šia technologija, norint neprarasti darbo sutarties Kollewe, J. (2018).

Nepaisant susirūpinimo, ši technologija plinta ir populiarėja visame pasaulyje. Šiuo metu vieni iš siūlomų implantų yra grysti radijo dažnio atpažinimo (RFID) technologija. Kita alternatyva yra artimojo lauko ryšio (NFC) implantai. RFID implantas gali būti naudojamas paprastam duomenų, pvz., sąskaitų numerių / patvirtinimo, perdavimui ir yra nuskaitomas nedideliu atstumu radijo bangomis, kurias priima skaitytuvas Hoffman, C. (2016). NFC implantas išsivystė iš RFID technologijos ir yra belaidis duomenų perdavimo būdas, kai vienas lustas aptinka ir leidžia kitam arti esančiam perduoti nedidelius duomenų kiekius Faulkner, C. (2017).

Visų biometrinių sistemų veikimas yra grindžiamas autentiškumo nustatymu ir visada susideda iš įrašymo, bei autentiškumo nustatymo etapų. Įrašymo etape naudotojas registruojamas naudojant gautus biometrinius duomenis. Autentiškumo nustatymo etape naudotojas atpažįstamas lyginant gyvą biometrinių požymių su saugomais biometriniais duomenimis. Biometrinės sistemos įprastai susideda iš

keturių pagrindinių modulių Jain, A. K., Ross, A. ir Prabhakar, S. (2004). Šie keturi moduliai yra būtini bet kurioje biometrinėje sistemoje, norint surinkti ir apdoroti neapdorotus biometrinius duomenis, juos paverčiant naudinga informacija:

- **Jutiklio modulis** – šio tipo modulyje neapdoroti biometriniai duomenys yra fiksuojami jutikliu, nuskaitančiu biometrinį požymį, po to verčiami skaitmenine forma. Atlikus konvertavimą į skaitmeninę formą, šis modulis turimus duomenis perduoda į funkcijų išgavimo modulį.

- **Funkcijų ištraukimo modulis** – šiame modulyje yra apdorojami, jutiklio užfiksuoti neapdoroti duomenis, iš kurių sukuriamas biometrinis šablonas. Iš neapdorotų duomenų išskiriamos reikiamos savybės, kurioms įprastai reikalinga skirti daugiau dėmesio, nes esminės savybės turi būti išgaunamos optimaliausiu būdu. Modulis iš esmės pašalina galimus trukdžius iš įvesties mėginio ir perduoda mėginį į įvesties pavyzdį kitam moduliui.

- **Atitikmenų modulis** – šis modulis lygina įvesties pavyzdį su duomenų bazėje saugomais šablonais, panaudodamas atitikties algoritmą. Gautas rezultatas perduodamas sprendimų moduliui, kuris nusprendžia, priimti asmenį ar ne.

- **Sprendimo modulis** – priėmus atitikties balą iš atitikmenų modulio, jis palyginamas su atitikties rezultatu su iš anksto nustatyta saugumo riba. Šis modulis priima arba atmeta asmenį pagal iš anksto nustatatomą saugumo slenkstį. Jei atitikties balas yra didesnis nei iš anksto nustatytas saugumo slenkstis, asmuo yra patvirtinamas, priešingu atveju patvirtinimas atmetamas.

1.3. Biometrinių technologijų plėtra

Biometrinių technologijų plėtra palaipsniui tampa vis akivaizdesnė ir sutinkama įvairiose pramonės šakose, įskaitant kelionių ir pasienio kontrolę, sveikatos priežiūrą, teisėsaugą, nacionalinį saugumą. Remiantis „Marketsand Markets“ viešinama ataskaita (2022 m.), tikimasi, kad iki 2026 metų pasaulinė biometrinių technologijų rinka pasieks 74,5 mlrd. dolerių ir 2021-2026 m. numatomas plėtros prieaugis sieks 19,5 %. Vienas iš naujausių biometrinių technologijų plėtros pasiekimų yra veido atpažinimo technologijos naudojimas. Kurio tikslas pasitelkiant atpažinimo technologijoje naudojamus algoritmus išanalizuoti ir sulygtinti asmens veido bruožus su esama informacija duomenų bazėse, taip siekiant patvirtinti asmens tapatybę. Remiantis „Grand View Research“ ataskaita (2021 m.), tikimasi, kad iki 2027 m. pasaulinės veido atpažinimo rinkos dydis pasieks 12,92 mlrd. dolerių, o nuo 2020 m. iki 2027 m. augs iki 16,6 %. Iš kitų biometrinių technologijų ataskaitoje išskiriama biometrinių dėvimųjų prietaisų naudojimas. Biometriniai dėvimi prietaisai suteikia galimybes sekti ir stebėti fiziologinius ir elgsenos duomenis, pavyzdžiui, širdies ritmą, kraujospūdį ir miego režimą, taip suteikiant galimybes patvirtinti naudotojo tapatybę. Remiantis „Research And Markets“ ataskaita (2021 m.), tikimasi, kad iki 2026 m. pasaulinės biometrinių dėvimųjų prietaisų rinkos dydis ir toliau plėsis, bei pasieks 54,8 mlrd. dolerių ribą, o nuo 2021 m. iki 2026 m. naudojimas augs iki 21,8 %.

Biometrinės technologijos taip pat vis dažniau naudojamos finansų pramonėje autentifikavimo ir saugumo tikslais. Kaip pavyzdį galima paminėti „Mastercard“, kuri pristatė biometrinę kortelę, kurioje naudotojo tapatybei patvirtinti jau yra naudojami pirštų atspaudai (Mastercard, 2021 m.). Šia technologija siekiama suteikti naudotojams saugesnę ir patogesnę mokėjimo patirtį.

Pastaraisiais metais biometrinės technologijos vis labiau populiarėja ir pačioje Europoje, biometrinės sistemos diegia vis daugiau vyriausybinių ir privačių organizacijų. Vienas iš tokių pavyzdžių yra biometrinių duomenų naudojimas pasienio kontrolės sistemose, Europos šalių tarpe diegiamos biometrinės pasienio kontrolės sistemos, siekiant pagerinti saugumą ir padidinti pasienio kontrolės operacijų efektyvumą (Frost & Sullivan, 2019). Biometrinių technologijų naudojimas ir plėtra skverbiasi į įvairias pramonės šakas, pavyzdžiui, sveikatos priežiūros, bankininkystės ir transporto sritis.

Atsižvelgiant į vykstančią plėtrą Europos Sąjunga įgyvendino taisykles, kuriomis siekiama užtikrinti, kad biometriniai duomenys būtų tvarkomi ir saugomi saugiai, ir apsaugotų asmenų privatumą. Pavyzdžiui, Bendrajame duomenų apsaugos reglamente (BDAR) pateikiamos biometrinių duomenų rinkimo, saugojimo ir tvarkymo ES gairės (ES BDAR, 2018). Europos Komisija aktyviai skatina biometrinių technologijų plėtrą ir naudojimą. Komisija taip pat finansavo keletą su biometrija susijusių mokslinių tyrimų projektų, pavyzdžiui, biometrinių duomenų vertinimo ir testavimo (BEAT) platformą, kuria siekiama pagerinti biometrinių sistemų tikslumą ir patikimumą (European Commission, n.d.).

1.4. Biometrinių technologijų sąlygojamos grėsmės

1.4.1. Grėsmių sritys

Plėtojantis biometrinėms technologijoms, atsiranda ir papildoma grėsmių tikimybė asmens duomenų apsaugai užtikrinti. Atsižvelgiant į naudojamų biometrinių duomenų specifiką, bei taikomus saugojimo metodus, vis dažniau pastebima įvairių bandymų kenkėjiškais tikslais paveikti biometrinės apsaugos sistemas, naudojantis atrastais sistemų pažeidžiamumais, duomenų klastojimo metodikomis, naudojant suklastotą arba nukopijuotą biometrinę informaciją, ar pasinaudojant esančiomis teisinio reguliavimo spragomis. Dažniausiai pasitaikančias biometrinių technologijų sąlygojamas grėsmes galima suskirstyti į šešias pagrindines sritis:

1. Biometrinių duomenų saugumo pažeidimai: viena iš pagrindinių biometrinių duomenų valdymo grėsmių yra duomenų saugumo pažeidimų rizika. Žinoma, kad biometriniai duomenys yra labai jautrūs ir gali būti naudojami asmenims identifikuoti taip, kaip tradiciniai slaptažodžiai ar „PIN“ kodai. Todėl jei biometriniai duomenys patenka į netinkamas rankas, jie gali būti panaudoti tapatybės vagystei ar kitiems piktavališkiems tikslams. Pavyzdžiui, 2021 m. dėl populiarus pirštų atspaudų

skaitytuvų gamintojo duomenų saugumo pažeidimo buvo atskleisti daugiau nei milijono žmonių biometriniai duomenys. (Campbell, 2021 m.)

2. Piktnaudžiavimas biometriniais duomenimis: grėsmė pasireiškianti, per prieigą prie biometrinių duomenų valdymo turinčius subjektus ir galimybe piktnaudžiauti prieinamais duomenimis. Tai gali būti vyriausybės agentūros, teisėsaugos institucijos, ar net darbdaviai. Kai kuriais atvejais biometriniai duomenys gali būti pasitelkiami ir naudojami asmenims sekti be jų žinios ar sutikimo. Pavyzdžiui, Kinijoje vyriausybė naudojo veido atpažinimo technologiją uigūrų musulmonų populiacijai sekti ir stebėti. (Human Rights Watch, 2020 m.)

3. Netikslūs duomenys: biometriniai duomenys turi tikimybę ne visada būti priimti tiksliai, todėl atsiranda klaidingai teigiamų, arba klaidingai neigiamų autentifikavimo atvejų tikimybė. Tai gali būti ypač problemiška tais atvejais, kai biometriniai duomenys naudojami priimant svarbius sprendimus, pavyzdžiui, suteikiant teisę patekti į saugias vietas, arba nustatant teisę gauti valstybės išmokas. Dėl netikslių duomenų asmenims gali būti nepagrįstai atsisakyta suteikti prieigą ar išmokas arba, atvirkščiai, jiems gali būti suteikta prieiga prie slaptos informacijos ar vietų, į kurias jie neturėtų patekti. (Munir ir Siddique, 2021)

4. Reguliavimo trūkumas: yra vienas iš biometrinių duomenų valdymo iššūkių, traktuojamas kaip reguliavimo ir standartizavimo trūkumas. Skirtingai nei kitų tipų asmens duomenų atveju, nėra aiškių gairių ar įstatymų, reglamentuojančių biometrinių duomenų rinkimą ir naudojimą. Dėl šio reguliavimo trūkumo gali atsirasti nenuoseklumų, klaidų renkant ir naudojant duomenis, o tai gali lemti galimus pažeidimus ar jų netinkamą naudojimą. Todėl yra svarbus, pastovus ir savalaikis biometrinių technologijų plėtros stebėjimas. Kuris būtų pagrįstas tikslingu teisiniu koordinavimu, sprendžiant kylančias problemas ir galimas rizikas, parengiant aiškius biometrinių duomenų valdymo standartus.

5. Pažeidžiamumas kibernetinių atakų atžvilgiu: biometriniai duomenys taip pat yra pažeidžiami kibernetinių atakų, kurios gali pakenkti duomenų saugumui. Kibernetiniai nusikaltėliai gali bandyti įsilaužti į biometrinių duomenų bazines, kad pavogtų ar pakeistų saugomus asmens duomenis, arba gali naudoti socialinės inžinerijos metodus, taip siekiant gauti prieigą prie duomenų, per įgaliotus naudotojus. Kadangi biometriniai duomenys naudojami vis plačiau, organizacijoms svarbu teikti pirmenybę kibernetinio saugumo priemonėms, kad apsisaugotų nuo šio tipo grėsmių.

6. Privatumas: biometrinių duomenų valdymas kelia didelį susirūpinimą ir dėl privatumo asmens atžvilgiu. Asmenims gali būti nemalonu rinkti ir naudoti savo biometrinius duomenis, ypač jei jie nėra išsamiai informuoti apie tai, kaip jie bus naudojami ir kas galės jais naudotis. Be to, kyla pavojus, kad biometriniai duomenys gali būti naudojami asmenims sekti be jų žinios, ar sutikimo. Kadangi biometriniai duomenys tampa vis labiau paplitę, svarbu, kad organizacijos skaidriai informuotų apie savo duomenų rinkimo praktiką ir teiktų pirmenybę asmens teisėms į privatumą.

1.4.2. Atakos biometrinėse sistemose

Sparčiai augant biometrinių sistemų populiarumui, vis labiau plinta ir atakų orientuotų į šias sistemas atvejų kiekiai. Kaip rodo naujausi atlikti tyrimai, biometrinių atakų skaičius kasmet tendencingai auga, o tai kelia grėsmę biometrinių sistemų saugumui ir asmens duomenų privatumui.

Viena iš naujausių biometrinių atakų tendencijų yra susijusi su „deepfake“ technologija. Ši technologija yra dirbtinio intelekto (DI) principu grysta technologija, kuri leidžia manipuliuoti vaizdo arba garso įrašais taip, kad jie atrodytų tikri. Ši technologija gali būti naudojama biometrinių sistemų atakoms vykdyti, kai sukuriama netikri biometriniai duomenys, kurie vėliau gali būti panaudojami kaip autentiški, biometrinių sistemų autentifikacijos proceso metu (Jain, Ross, ir Nandakumar, 2016). Pasak autorių Ahire ir Patil (2019), technologija yra viena iš naujausių biometrinių atakų tendencijų. Teigiama, kad dažniausiai su šia technologija vykdomos atakos yra siekiant apgauti veido atpažinimo sistemas, tačiau gausu atveju kai yra imituojami ir realūs asmenys. Šio tipo atakos gali būti labai pavojingos, kadangi technologija suteikia galimybes kurti netikrus vaizdo įrašus, kuriuose atrodo, kad žmogus dalyvauja tam tikroje veikloje ar atlieka tam tikrus veiksmus, kai realybėje viskas gali būti priešingai. Tokiu būdu, „deepfake“ atakos ne tik gali kelti grėsmę biometrinių sistemų saugumui, bet ir padaryti didelę žalą asmens reputacijai.

Kita nauja biometrinių atakų tendencija, kaip pabrėžia autoriai Ahire ir Patil (2019) apima stenografijos naudojimą biometrinių atakų metu. Stenografija yra slaptų pranešimų siuntimo technologija, kuri leidžia slapta paslėpti informaciją tarp kitų duomenų. Ši technologija gali būti naudojama biometrinių atakų metu, kad apgavikai galėtų paslėpti biometrinius duomenis tarp kitų duomenų ir perduoti juos per ryšio kanalą. Tai gali suteikti galimybę gauti neteisėtą prieigą prie biometrinių duomenų ir taip paveikti biometrinių sistemų saugumą.

Dar viena nauja tendencija yra susijusi su biometrinių sistemų atakomis naudojant neuroninius tinklus. Tyrimai rodo, kad neuroniniai tinklai gali būti naudojami kaip ataka į biometrinių sistemų duomenų bazę. Naudojant neuroninius tinklus, apgavikai gali sugeneruoti daugybę netikrų biometrinių duomenų, kurie gali būti naudojami autentifikuojant save biometrinių sistemų procese. Šio tipo ataka yra labai pavojinga, nes apgavikai gali lengvai apgauti biometrinių sistemų saugumo mechanizmus ir prieiti prie jų duomenų Kumar, H. (2021).

Autorių Latha U. ir Rameshkumar K. (2013) atliktame tyrime nurodoma, kad biometrinės sistemos turi aštuonis atakų tipus, kurių pagrindu gali būti inicijuojamos atitinkamos atakos. Šie atakos tipai gali būti skirstomi į dvi kategorijas: tiesiogines arba netiesiogines:

Tiesioginės atakos – yra viena iš pagrindinių biometrinės apsaugos sistemų grėsmių. Tokio tipo atakos yra bandymas tiesiogiai panaudoti kenkėjiškas priemones, kad būtų perduoti neteisėti signalai biometrinėms sistemoms, o tai gali lemti neteisėtą prieigą prie informacijos, kuri yra saugoma šiose

sistemose. Šio tipo atakos nereikalauja specifinių žinių apie sistemos veikimą, naudojamą atitikmens algoritmą, funkcijų vektorių formatą. Remiantis „Forbes“ žurnalo straipsniu, tiesioginės atakos biometrinėse sistemose yra bandymas tiesiogiai panaudoti kenkėjiškas priemones, kad būtų perduoti neteisėti signalai biometrinėms sistemoms (Shekhar, 2021). Šio tipo ataka gali būti įgyvendinama naudojant daugybę priemonių, tokių kaip padirbtos biometrinės charakteristikos, suklustoti biometriniai duomenys ar netgi fiziniai įsilaužimai į pačias priemones. Pavyzdžiui, gali būti panaudotas suklustotas pirštų atspaudas, kad būtų lengviau patekti į saugias patalpas ar netgi išgauti asmeninę informaciją (Shekhar, 2021). Tiesioginės atakos biometrinėse sistemose gali padaryti didelę žalą organizacijoms ir asmenims, kurie pasitiki biometrinės apsaugos sistema. Tokios atakos gali lemti asmens duomenų vagystę, finansinius nuostolius ar netgi fizinę žalą, jei yra naudojamos tam tikros rūšies biometrinės apsaugos sistemos, tokios kaip veido atpažinimas, kurių tikslumas yra kritiškas (Goldschmidt, 2021). Tiesioginė atakos įprastai apima tik vieno tipo ataką, kuri yra vadinama sensorine ataka:

- **1 tipo sensorinė ataka:** suprantama kaip prieš jutiklį vykdoma ataka, apima suklustotą biometrinį požymį, pavyzdžiui, dirbtinio piršto ar veido atvaizdo, pateikimą jutikliui, siekiant apeiti atpažinimo sistemas (Jain et al., 2016). Užpuolikai taip pat gali fiziškai sugadinti atpažinimo sistemą ir apkrauti sistemą netikromis prieigos užklausomis. Tokio tipo atakas yra paprasta vykdyti, nes joms nereikia specialių žinių apie sistemos veikimą, o skaitmeniniai saugumo mechanizmai, pavyzdžiui, vandens ženklai ir kriptografija, jutiklio lygmeniu nėra naudojami. Jutikliai negali atskirti suklustotų ir tikrų asmens požymių, juos galima lengvai apgauti naudojant sintetinius pirštų atspaudus ir veido atvaizdus (Li, Z. ir kt., 2019).

Netiesioginės atakos - įvykdyti sėkmingas atakas, reikalinga informacija apie autentifikavimo sistemos vidinį veikimą. Šio tipo atakos apima likusius septynis atakos tipus, į kuriuos gali būti nukreipta biometriniais duomenimis pagrįsta autentifikavimo sistema (Damer, 2021):

- **2 tipo ataka:** suprantama kaip jutiklio neapdorotų biometrinį duomenų siuntimas, požymių išskyrimo moduliui, išankstiniam apdorojimui. Duomenys siunčiami ryšio kanalu, tarp jutiklio ir požymių išskyrimo modulio yra perimami, kad būtų galima pavogti biometrinį požymį, siekiant kur nors jį išsaugoti. Tuomet išsaugotas biometrinis požymis yra perduodamas atgal į požymių išskyrimo modulį, taip siekiant apeiti jutiklį, kas yra vadinama atkūrimo ataka (Damer, 2021).

- **3 tipo ataka:** ataka pasireiškia funkcijų ištraukimo modulio pažeidžiamume ir vadinama „Funkcijų ištraukimo modulio ataka“. Procese, kai jutiklis perduoda neapdorotus biometrinius duomenis į funkcijų ištraukimo modulį, apgavikas manipuliuoja moduliu, kad būtų sukurta terpė, kuri generuotų įsibrovėlio pasirinktas savybių vertes, o ne iš pradinių jutiklio gautų duomenų sugeneruotais savybių rinkiniais (Sahoo, G., ir Gupta, B. B. 2013).

- **4 tipo ataka:** ataka pasireiškia, kai įsibrovėlis prieina prie šaltinio, kuris gali suteikti informaciją apie biometrinių įrenginių arba jos komponentus, ir tuo būdu gali manipuliuoti biometriniais duomenimis arba sukurti dirbtinę tapatybę (Sahoo, G., ir Gupta, B. B. 2013).

- **5 tipo ataka:** ataka vyksta, kai yra manipuliuojamas atitikmens modulis, generuojant dirbtinai aukštą atitikimo balą, nepriklausomai nuo funkcijų rinkinio, gauto iš įvesties, taip siekiant apeiti biometrinio autentifikavimo sistemą (Sahoo, G., ir Gupta, B. B. 2013).

- **6 tipo ataka:** apima bandymą įsilaužti į saugomą duomenų bazę, keičiant esamus biometrinius šablonus arba pridėdant naujus. Šios atakos yra sudėtingos, nes biometriniai šablonai yra apsaugoti nuo pažeidimų skaitmeniniais mechanizmais, tokiais kaip steganografija, vandenženklis ir kt. Ko pasėkoje norint sėkmingai atakuoti sistemą, reikalingos išsamesnės žinios apie vidinę sistemos struktūrą ir jos veikimą.

- **7 tipo ataka:** atakos scenarijus yra įmanomas tik tuo atveju, kai biometrinis šablonas perduodamas per ryšio kanalą tarp sistemos duomenų bazės ir atitikmens modulio. Apgavikas gali bandyti pakeisti arba sugadinti šablono turinį, sulaikydamas ryšio kanalą, kad pasiektų savo tikslus.

- **8 tipo ataka:** apima bandymus manipuliuoti suderinimo modulio deklaruojamais rezultatais. Puolėjas gali sukurti klaidingus arba iškraipytus rezultatus, kurie yra perduodami per ryšio kanalą tarp atitikimo modulio ir programos įrenginio. Tokiu būdu, jis gali bandyti pakeisti pradinį suderinimo modulio sprendimą, priversti sistemą priimti ar atmesti tam tikrus veiksmus.

Atsižvelgus į šiuos aštuonis atakų tipus, galima daryti prielaidą, kad palankiausia yra atakuoti šablonus saugomus duomenų bazėje. Tai suteikia galimybes šablonus sugadinti, į duomenų bazę įtraukiant naujus, esant poreikiui esamus modifikuoti, ar net juos pašalinti iš duomenų bazės.

1.4.3. Grėsmės privatumą išsaugančioms biometrinėms autentifikavimo sistemoms

Įvairių atakų taikymas prieš privatumą išsaugančias sistemas, siekiant išgauti informaciją apie vartotojo biometrinius požymius ar tapatybę, iškelia papildomas grėsmes. Norint užtikrinti asmens duomenų apsaugą ir privatumą, būtina nagrinėti taikomų atakų strategijas ir tikslus, kurie gali turėti didelę įtaką šių problemų sprendimui, ypač atsižvelgiant į tai, kad biometriniai šablonai yra neatšaukiami. Pagal Abate ir kt. (2018) atliktą tyrimą, biometrinės autentifikavimo sistemos gali kelti grėsmę privatumui. Remiantis atlikto tyrimo rezultatais, biometrinių duomenų surinkimas ir saugojimas yra kritinės svarbos, dėl šių sistemų patikimumo klausimo. Taip pat, tyrime pabrėžiama, kad biometrinių duomenų naudojimas kitais tikslais, nei autentifikavimas, gali sukelti rimtas privatumo problemas Abate ir kt., (2018). Bhatnagar ir Jain (2019) atliko tyrimą, kuris parodė, kad biometrinės autentifikavimo sistemos turi trūkumų, susijusių su privatumu. Remiantis jų išvadomis, biometrinių duomenų rinkimas, saugojimas ir perdavimas turi būti tvarkomi kruopščiai, kad būtų išvengta galimų privatumo pažeidimų. Todėl norint sukurti veiksmingą priešinimosi modelį, reikia

išskirti keturias pagrindines grėsmes, kurios gali paveikti asmens duomenų privatumą, kai naudojamos biometrinės autentifikavimo sistemos Joseph M., Michael K., ir Stephen K. (2019):

1. Biometrinio mėginio atkūrimas – yra procesas, kai įsilaužėlis bando sukurti naują biometrinį šabloną, kuris bus priimtas autentifikavimo serveryje. Tai daroma siekiant apgauti biometrinės apsaugos sistemas ir patekti prie apribotos informacijos. Šio tipo atakos rezultatai yra panašūs į atskaitos atkūrimo ataką, tačiau yra keletas svarbių skirtumų. Vienas iš pagrindinių skirtumų yra tai, kad sukurtas atitikimo šablonas gali neatitikti tikrojo vartotojo biometrinio šablono. Dėl to įsilaužėlis gali atkurti mažiau informacijos apie vartotojo privačią informaciją ir tam tikras fizines savybes. Taip pat, dėl šio skirtumo, biometrinio mėginio atkūrimo ataka gali būti mažiau efektyvi, nes ji priklauso nuo įsilaužėlio sugebėjimo sukurti pakankamai tikslų biometrinį šabloną, kuris būtų priimtas autentifikavimo serveryje.

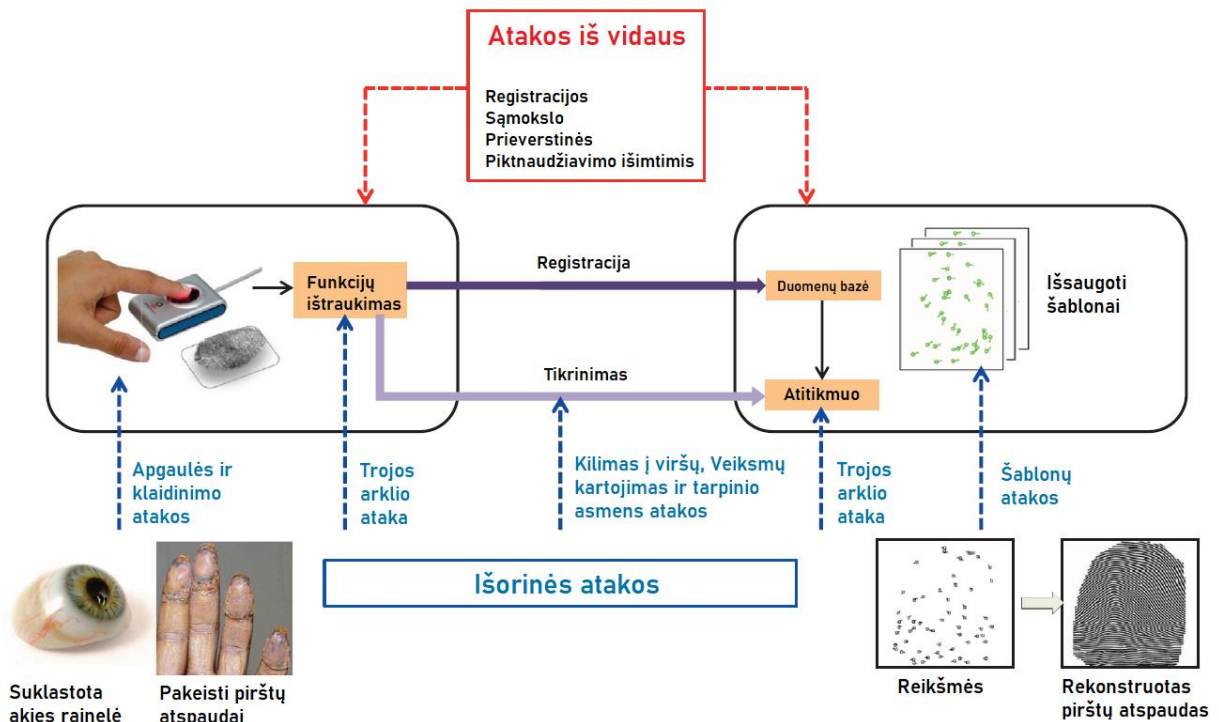
2. Biometrinės atskaitos atkūrimas – yra procesas, kai neteisėtas asmuo, paprastai vadinamas įsilaužėliu, sugeba atkurti biometrinę atskaitą neįslaptintame formate. Ši atakos rūšis yra viena iš pavojingiausių, kadangi įsilaužėlis, atkūręs biometrinį šabloną, gali gauti neautorizuotą prieigą prie bet kokios sistemos, kurioje šis šablonas naudojamas kaip atskaitos taškas. Be to, šiame procese įsilaužėlis gali surinkti konfidencialią informaciją apie vartotoją, įskaitant ir saugomas fizines savybes.

3. Vartotojo atsekamumas – yra situacija, kai neleistinas asmuo seka vartotojo autentifikavimo veiksmus skirtingose aplikacijose. Jei tokia stebėjimo ataka pasiseka, tai gali sukelti kryžminį nustatymą, kaip naudotojų profilių sukūrimą ir pan. Šio tipo atakos gali kelti rimtą grėsmę naudotojų privatumui ir saugumui, nes neteisėtos šalies galimybė stebėti naudotojų autentifikavimo procesus, gali lemti galimybes sukurti detalius profilius, atskleisti jų elgesio modelius ir netgi sekti juos realiu laiku. Tokios informacijos gavimas gali būti panaudotas piktnaudžiavimui, įskaitant tapatybės vagystę, sukčiavimą ar sabotazo atvejus.

4. Naudotojo išskirtinumas – įsilaužėlio tikslas yra užmegzti ryšį tarp biometrinio šablono ir naudotojo tapatybės. Kai šis ryšys pažeidžiamas, gali būti atskleista labiau konfidenciali informacija, dėl ko dažnai sumažėja sistemos anonimiškumas ir kyla atitinkamos saugumo problemos. Tokios pažeidimo atakos gali kelti grėsmę naudotojų privatumui, nes įsilaužėlis gali atskleisti jautrią informaciją apie naudotoją, kaip asmens duomenis, elgesio modelius ar fizines savybes. Norint apsaugoti sistemų naudotojus nuo šios atakos rūšies, būtina imtis prevencinių priemonių, tokių kaip anonimizavimo technologijos, kriptografijos taikymo duomenų apsaugai ir tinkamų saugumo protokolų naudojimo.

Svarbu suprasti, kad biometrinių sistemų įdiegimas nėra visiškas sprendimas saugumo užtikrinimui, ir turėtų būti laikomos papildomomis priemonėmis. Tam, kad biometrinės sistemos veiktų maksimaliai efektyviai, reikalingas jų kruopštus testavimas ir derinimas su kitomis apsaugos priemonėmis, taip užtikrinant maksimalų atitinkamą saugumo lygį. Nors vienas iš pagrindinių

biometrinių sistemų tikslų yra orientuotas į aplikacijų ir programų saugumo užtikrinimą, siekiant išvengti neautorizuotos prieigos galimybių, reikia atsižvelgti ir į tai, jog šios sistemos tam tikrais atvejais negarantuoja absoliutaus saugumo ir privatumo užtikrinimo, kaip jau buvo aptarta praeituose skirsniuose. Biometrinės sistemos taip pat gali patirti išorinio ir vidinio pobūdžio atakas, kurios gali turėti didesnę ar mažesnę poveikį pačių sistemų saugumui, bei saugomų duomenų integralumui (žr. 1 pav.).



Šaltinis: adaptuotas pagal A.K. Jain et al., 2016

1 pav. Autentifikavimo sistemų atakos

Paveikslėlyje pateikiami galimų atakų scenarijai, kuriais gali būti pažeistos biometrinės sistemos. Nors dauguma saugumo grėsmių yra bendro pobūdžio, apimančios bet kokią autentifikacijos metodu grįstą sistemą. Sukčiavimo atvejų problemos, kaip padirbtų biometrinių požymių pristatymas ir atakos šablonų taikymas duomenų bazei, ar siekis atkurti pradinę biometrinių duomenų informaciją, taip atliekant kryžminį atitikimą, yra specifinė grėsmė apimanti tik biometrinės sistemas.

Nors daugelis pasitelkiamų atakų prieš biometrinės sistemas, kaip trojos arklys, perregistravimas ar tarpininkavimo atakos, yra bendros visoms autentifikacijos sistemoms ir gali būti užkardomos pasinaudojant idėjomis iš kitų esamų saugių slaptažodžių autentifikavimo metodikų, yra dvi saugumo spragos, kurios yra specifinės būtent biometrinėms sistemoms. Viena iš jų yra sukčiavimo problema, kai biometrinis jutiklis yra pateikiamas su padirbtu biometrinio požymiu Marcel, S., Nixon, M., & Li, S. Z. (2014). Sukčiavimo aptikimas yra kritinis ir svarbus reikalavimas, ypač nesupervizuojamose aplikacijose, kuriose naudotojo buvimas nėra stebimas. Autoriai S. Yoon, J. Feng ir A.K. Jain, 2012

metais atliktame tyrime teigia, kad kitas svarbus pavojus yra sistemos saugumas ir naudotojų privatumo grėsmės, kylančios, dėl biometrinių šablonų informacijos nutekėjimo atakų vykdymo metu į šablonų duomenų bazę. Tyčinis biometrinių požymių keitimas siekiant išvengti identifikavimo yra besiformuojanti grėsmė kai kurioms esamoms aplikacijoms, kaip tarptautinio sienų kirtimo kontrolė ir panašiai. Svarbu pabrėžti, kad biometrinių sistemų saugumas ir naudotojų privatumo klausimai yra svarbios visuomenės suvokimo problemos. Šios problemos gali kelti grėsmę biometrinių sistemų sėkmei, jei jos nėra išsamiai aptariamoms. Sukčiavimo aptikimas paprastai apima specifinių požymių ir savybių patikrinimą, kurie parodo, ar asmuo yra gyvas. Patikrinimas, gali apimti pulsą, akies mirksėjimo dažnį ir kitas galimas savybes, bei požymius. Todėl šis procesas yra vadinamas gyvumo aptikimu Marasco, E., ir Ross, A. (2015). Norint, kad gyvumo aptikimo metodai pasiteisintų praktikoje, realiu laiku ir pasižymėtų aukštu tikslumu, turi būti užtikrinama galimybė atpažinti sukčiavimo bandymus, nesukeliant papildomų nepatogumų naudotojams, turintiems teisėtą prieigą. Nors sukčiavimo aptikimo technikos paprastai yra projektuojamos konkreitiems biimetriniams modalumams, juos galima suklasifikuoti į tris pagrindines kategorijas Nixon, K. A., ir Rowe, R. K. (2005):

- **Pirmoji kategorija** – apima gyvo asmens fiziologinių savybių matavimą, įskaitant kraujo pulsą, bei slėgį, prakaitavimą, spektrinius ar optinius žmogaus odos ar audinių rodiklius, elektrinius, šiluminių charakteristikų ir raumenų, odos deformacijas.
- **Antroji kategorija** – pagrįsta identifikuojant savanoriškus ar nekontroliuojamus žmogaus veiksmus, tokius kaip svyravimai, mirksėjimas, akių, galvos ar kūno judesiai.
- **Trečioji kategorija** – vadinama tam tikros užduoties teisingo atlikimo metodu, kai sistemoje prašoma naudotojo atlikti atitinkamą veiksmą, kuris po to yra tikrinamas ir pamatuojamas jo atlikimo tikslumas.

Kad būtų sudarytos sąlygos užtikrinti priimtina saugumo lygį, autentifikavimo sistemose, naudotojams gali būti pateiktas prašymas atlikti papildomą veiksmą. Veiksmas gali apimti, prašymą pasakyti atsitiktinai sugeneruotą frazę ar tekstą sistemose naudojančiose garso patvirtinimą, arba pakeisti veido išraišką (pvz., šypsantis ar raukiantis) veido bruožų patvirtinimo sistemose Diaz, J. (2021). Kitas svarbus aspektas yra apgaulės aptikimo tikslumo ir naudotojų patogumo santykio pasirinkimas. Norint minimalizuoti saugumo ir privatumo rizikas, susijusias su biimetrinėmis sistemomis, būtina apsaugoti biimetrinius šablonus, saugomus sistemos duomenų bazėje. Idealesnis sprendimas būtų nesaugoti jokios biimetrinės informacijos duomenų bazėje, o apsiriboti tik biimetrinių savybių pavertimu atsitiktiniais raktais Jain, Ross, ir Nandakumar, 2016 . Tačiau tai reikalauja tokio modelio taikymo, kuris būtų įvairiapusiškas naudotojų skirtumams ir tuo pačiu unikalūs kiekvienam naudotojui. Praktiškesnis ir patikimesnis sprendimas yra biimetrinių šablonų

transformavimas į saugius šablonus, atitinkančius tris specifinius reikalavimus Jain, Ross, ir Nandakumar, 2016):

- **Nekintamumas** – saugomas šablonas turėtų būti sunkiai apskaičiuojamas, siekiant maksimaliai apriboti galimybę iš jo atkurti biometrinius požymius. Tai užkardytų galimybę atkurti biometrinius požymius iš šablono, arba sukurti fizinių biometrinio požymio klastočių.

- **Nesusiejamumas** – turėtų būti įmanoma iš tų pačių biometrinių duomenų sukurti kelis saugius šablonus, kurių nebūtų įmanoma susieti tarpusavyje. Ši savybė biometrinei sistemai leistų atšaukti ir iš naujo išduoti naujus šablonus, kai duomenų bazė tampa pažeidžiama, taip užtikrinant, kad kryžminis palyginimas tarp duomenų bazių būtų neįmanomas, tokiu būdu išsaugant naudotojo privatumą.

- **Diskriminavimas** – saugus šablonas kuris neturėtų turėti įtakos biometrinės sistemos atpažinimo tikslumui.

1.5. Asmens duomenų apsaugos reglamentavimas

Šiuolaikiniame skaitmeniniame pasaulyje asmens duomenų rinkimas, tvarkymas ir perdavimas yra esminė verslo sektoriaus operacijų dalis. Tačiau, vis dažniau naudojant asmens duomenis, atsiranda poreikis nustatyti ir reglamentuoti tarptautines taisykles, skirtas asmens privatumui apsaugoti. Šiais reglamentais siekiama užtikrinti, kad asmenys galėtų kontroliuoti savo asmens duomenis, o organizacijos būtų atsakingos už šių duomenų apsaugą. Šiuo atžvilgiu galima išskirti ir palyginti du svarbius tarptautinius reglamentus: Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (BDAR) ir Jungtinių Amerikos Valstijų Kalifornijos vartotojų privatumo įstatymas (CCPA):

- **Bendrasis duomenų apsaugos reglamentas (BDAR)** – yra išsamus privatumo apsaugos reglamentas, kuris Europos Sąjungoje įsigaliojo 2018 m. gegužės mėn. Bendrasis duomenų apsaugos reglamentas pakeičia Duomenų apsaugos direktyvą 95/46/EB ir turi atitinkamų pasekmių organizacijoms, kurios ES tvarko asmens duomenis. Vienas iš svarbiausių BDAR aspektų yra tas, kad juo išplečiama teritorinė ES duomenų apsaugos teisės taikymo sritis. BDAR taikomas visoms organizacijoms, nepriklausomai nuo jų buvimo vietos, kurios tvarko ES piliečių asmens duomenis. Tai reiškia, kad bet kuri organizacija, tvarkanti ES piliečių asmens duomenis, privalo laikytis BDAR, nepriklausomai nuo to, kur organizacija yra įsikūrusi.

Bendrasis duomenų apsaugos reglamentas suteikia asmenims atitinkamas teises, susijusias su jų asmens duomenimis. Pavyzdžiui, asmenys turi teisę susipažinti su savo asmens duomenimis, teisę reikalauti, kad jų duomenys būtų ištrinti, ir į teisę nesutikti, kad jų duomenys būtų tvarkomi. Šiomis teisėmis asmenims suteikiama didesnė jų asmens duomenų kontrolė ir jie gali geriau kontroliuoti, kaip organizacijos naudoja jų duomenis.

Pagal BDAR organizacijos privalo užtikrinti, kad asmens duomenys būtų tvarkomi teisėtai, sąžiningai ir skaidriai. Tai reiškia, kad organizacijos, prieš tvarkydamos asmens duomenis, privalo gauti galiojančią asmenų sutikimą. Organizacijos taip pat privalo suteikti asmenims aiškią informaciją apie duomenų tvarkymo tikslą ir kaip duomenys bus naudojami. Be to, organizacijos turi įgyvendinti tinkamas technines ir organizacines priemones, kad apsaugotų asmens duomenis nuo neteisėtos prieigos, atskleidimo ar netinkamo naudojimo.

Remiantis BDAR biometriniai duomenys yra laikomi neskelbtiniais asmens duomenimis, todėl jų tvarkymui taikomos griežtesnės taisyklės. Pagal BDAR reikalaujama, kad biometriniai duomenys būtų tvarkomi teisėtai, sąžiningai ir skaidriai. Prieš rinkdamos ir tvarkydamos biometrinius duomenis, organizacijos privalo gauti aiškų asmenų sutikimą. Be to, organizacijos privalo suteikti asmenims aiškią informaciją apie duomenų tvarkymo tikslą ir kaip duomenys bus naudojami. Organizacijos taip pat turi įgyvendinti tinkamas technines ir organizacines priemones, kad apsaugotų biometrinius duomenis nuo neteisėtos prieigos, atskleidimo ar netinkamo naudojimo. Galiausiai, organizacijos turi užtikrinti, kad biometriniai duomenys nebūtų saugomi ilgiau nei būtina.

Vienas iš svarbiausių BDAR aspektų – yra sugriežtintos sankcijos už reikalavimų nesilaikymą. Organizacijoms, kurios nesilaiko BDAR reikalavimų, gali būti skiriama bauda iki 4 % jų pasaulinių metinių pajamų arba 20 mln. eurų, atsižvelgiant į tai, kuri suma yra didesnė. Palyginti su ankstesne Duomenų apsaugos direktyva, pagal kurią didžiausios galimos baudos buvo daug mažesnės, tai yra gerokai didesnės baudos.

Europos Sąjungoje. Remiantis „Cisco“ atlikto tyrimo duomenimis, dėl BDAR padidėjo informuotumas apie duomenų privatumą ir organizacijos pradėjo daugiau dėmesio skirti duomenų apsaugai. Be to, dėl BDAR organizacijose padaugėjo duomenų apsaugos pareigūnų (DAP). DAP yra atsakingi už tai, kad organizacijos laikytųsi BDAR ir atsakytų į asmenų užklausas, dėl duomenų privatumo Cisco, (2019).

- **Kalifornijos vartotojų privatumo įstatymas (angl. California Consumer Privacy Act, CCPA)** – yra privatumo apsaugos reglamentas, kuris Jungtinėse Amerikos Valstijose įsigaliojo 2020 m. sausio 1 d. CCPA Kalifornijos gyventojams suteikia keletą teisių, susijusių su jų asmens duomenimis. Pavyzdžiui, asmenys turi teisę žinoti, kokie asmens duomenys apie juos renkami, teisę susipažinti su savo asmens duomenimis ir teisę reikalauti, kad jų duomenys būtų ištrinti. Be to, CCPA suteikia asmenims teisę atsisakyti parduoti savo asmens duomenis.

Pagal CCPA organizacijos privalo aiškiai ir matomai informuoti asmenis apie savo duomenų rinkimo praktiką. Be to, prieš parduodamos asmens duomenis, organizacijos privalo gauti teigiamą asmenų sutikimą. Organizacijos turi įgyvendinti pagrįstas saugumo priemones, kad apsaugotų asmens duomenis nuo neteisėtos prieigos, atskleidimo ar netinkamo naudojimo.

CCPA taip pat yra nuostatų, susijusių su biometrinių duomenų tvarkymu. Biometriniai duomenys apibrėžiami kaip „asmens fiziologiniai, biologiniai ar elgesio požymiai, įskaitant asmens DNR, kurie gali būti naudojami pavieniui arba kartu su kitais identifikaciniais duomenimis asmens tapatybei nustatyti“. Pagal CCPA reikalaujama, kad organizacijos, prieš rinkdamos ir tvarkydamos biometrinius duomenis, gautų teigiamą asmenų sutikimą. Organizacijos taip pat privalo aiškiai ir matomai informuoti asmenis apie savo duomenų rinkimo praktiką. Be to, organizacijos turi įgyvendinti pagrįstas saugumo priemones, kad apsaugotų biometrinius duomenis nuo neteisėtos prieigos, atskleidimo ar netinkamo naudojimo. Galiausiai, pagal CCPA reikalaujama, kad organizacijos asmens prašymu, ištrintų biometrinius duomenis.

CCPA daro didelį poveikį organizacijoms, kurios tvarko asmens duomenis Kalifornijoje. Remiantis „TrustArc“ atliktu tyrimu, 75 % apklaustų organizacijų teigė, kad CCPA padidino jų dėmesį duomenų privatumui, o 71 % organizacijų dėl CCPA padidino savo išlaidas duomenų privatumui. Dėl CCPA taip pat padaugėjo su privatumu susijusių laisvų darbo vietų, daugelis organizacijų įdarbino vyriausiuosius privatumo pareigūnus ir kitus privatumo specialistus TrustArc (2020).

Pasaulinės privatumo apsaugos tendencijos taip pat atsispindi pasaulio valstybių pastangose apsaugoti savo piliečių asmens duomenis. Pavyzdžiui, po to, kai Europos Sąjunga priėmė Bendrąjį duomenų apsaugos reglamentą (BDAR), kelios Europos Sąjungai nepriklausančios šalys, tokios kaip Brazilija, Japonija ir Pietų Korėja, priėmė panašias privatumo apsaugos taisykles. Be to, BDAR įsigaliojimas padidino teisinių ginčų skaičių, susijusių su privatumo klausimais, kuomet asmenys teikia skundus organizacijoms dėl BDAR nesilaikymo atvejų (Smith, 2020).

Apibendrinant galima teigti, kad BDAR ir CCPA yra du svarbūs tarptautiniai reglamentai, turėję didelį poveikį asmens duomenų privatumo užtikrinimui. Šiais reglamentais asmenims suteikiama didesnė jų asmens duomenų kontrolė, o organizacijoms atsakomybė už šių duomenų apsaugą. Nors BDAR ir CCPA numatyta tam tikra biometrinių duomenų privatumo apsauga, vis dar yra keletas iššūkių, kuriuos reikia išspręsti. Pavyzdžiui, biometriniai duomenys dažnai renkami be aiškaus asmenų sutikimo. Be to, biometriniai duomenys gali būti naudojami stebėjimo ir sekimo tikslais, todėl kyla susirūpinimas, dėl pilietinių laisvių ir asmens privatumo. Be to, į biometrinius duomenis gali būti įsilaužta ir gali būti pažeisti duomenų saugumo principai, o tai gali lemti tapatybės vagystę ir kitų formų kibernetinius nusikaltimus.

1.6. Biometrikos ir kibernetinio saugumo standartai

Kibernetinis saugumas tapo vienu svarbiausių klausimų organizacijoms ir vyriausybėms, ypač pastaraisiais metais, kai kibernetinių atakų mastai ir duomenų saugumo pažeidimų atvejai stipriai išaugo. Todėl organizacijoms atsirado poreikis, didinti investicijas į kibernetinio saugumo priemones,

siekiant apsaugoti savo turtą ir reputaciją. Biometrijos naudojimas asmenims autentifikuoti yra vienas iš perspektyviausių kibernetinio saugumo didinimo sprendimų (Doe, 2022).

Tačiau biometrinių duomenų naudojimas kibernetinio saugumo srityje taip pat kelia tam tikras rizikas, kaip biometrinių duomenų vagystės atvejai ir biometrinių sistemų klaidų, bei netikslumų rizikos. Remiantis praeituose skirsniuose aptarta informacija, galima daryti išvadą, kad biometrinis autentiškumo patvirtinimas nėra visiškai patikimas procesas ir gali būti sąlygojamas tam tikrų grėsmių. Iš išanalizuotos informacijos, pastebėjome, kad biometrinės sistemos gali būti pažeistos įsilaužėlių, kurie gali ne tik pavogti biometrinius duomenis, bet ir panaudoti juos apsimesdami teisėtais naudotojais. Taip pat išsiaiškinome, kad biometrinėse sistemose gali pasitaikyti klaidų ir netikslumų, dėl kurių gali atsirasti klaidingų teigiamų arba klaidingai neigiamų autentifikacijos rezultatų. Todėl siekiant sumažinti galimas rizikas, buvo sukurta keletas standartų, skirtų biometrinių sistemų saugumui ir patikimumui užtikrinti, parengiant biometrinių duomenų naudojimo kibernetinio saugumo srityje standartus. Šie standartai orientuoti į biometrinių sistemų saugumo ir patikimumo didinimą, apsaugą nuo galimos rizikos, susijusios su biometrinės autentifikacijos procesu. Šių standartų laikymasis teikia keletą privalumų. Pirma, tai padeda užtikrinti biometrinių sistemų saugumą ir patikimumą, apsisaugant nuo galimų rizikų, susijusių su biometriniu autentifikavimu. Antra, tai padeda užtikrinti biometrinių sistemų sąveiką, leidžiančią skirtingoms sistemoms keistis biometrine informacija. Galiausiai, tai padeda užtikrinti, kad biometrinės sistemos atitiktų teisinio reguliavimo reikalavimus, pavyzdžiui duomenų apsaugos įstatymus. Keletas svarbiausių išskirtinų biometrikos ir kibernetinio saugumo standartų yra:

- **ISO/IEC 19794-1** – standarte nustatytas duomenų formatas, skirtas keistis biometrine informacija. Jame apibrėžiama biometrinių duomenų struktūra ir pateikiamos biometrinės informacijos saugojimo, perdavimo ir apdorojimo gairės.
- **ISO/IEC 30107-1** – standarte nustatyti biometrinių duomenų pateikimo atakų aptikimo (PAD) reikalavimai. Jame apibrėžiamos pateikimo atakų, kuriomis bandoma apeiti biometrinių autentiškumo nustatymą pateikiant suklastotus biometrinius duomenis, aptikimo ir prevencijos procedūros.
- **NIST SP 800-76** – standarte nustatomi keitimosi biometriniais duomenimis formatų reikalavimai. Jame apibrėžiama biometrinių duomenų struktūra ir pateikiamos biometrinės informacijos saugojimo, perdavimo ir apdorojimo gairės.
- **NIST SP 800-63B** – standarte nustatyti skaitmeninės tapatybės gairių reikalavimai. Jame apibrėžiama skaitmeninių tapatybių, įskaitant biometrinių autentiškumo nustatymą, tikrinimo ir autentiškumo nustatymo tvarka.

- **FIDO2** – standarte nustatomi autentiškumo patvirtinimo, be slaptažodžio naudojant biometrinius ir kitus veiksnius reikalavimai. Jame apibrėžiamos procedūros, skirtos naudotojų autentiškumui nustatyti nenaudojant slaptažodžių ar PIN kodų.

Apibendrinant išvardintus standartus, juose pateikiamos biometrinių sistemų naudojimo kibernetinio saugumo srityje gairės ir geriausia praktika. Standartai padeda užtikrinti biometrinio autentiškumo nustatymo saugumą ir patikimumą, bei apsisaugoti nuo galimų rizikų, susijusių su biometrinių sistemų naudojimu.

2. TYRIMAI ATLIKTI BIOMETRINIŲ TECHNOLOGIJŲ NAUDOJIMO KONTEKSTE

Skyriuje aptariamos keturios temos, susijusios su biometrinių duomenų rinkimu, naudojimu ir pažeidžiamumu. Pirmoji tema, pateikta 2.1 skirsnyje, yra šalių reitingavimas pagal biometrinių duomenų rinkimą ir naudojimą. Šiame skirsnyje išryškinami pasaulinio požiūrio į biometrinių duomenų rinkimą skirtumai, ypač susiję su privatumo ir duomenų apsaugos įstatymais. Antroji tema, aptarta 2.2 skirsnyje, yra masinio biometrinių duomenų ir elgsenos stebėjimas ES valstybėse narėse. Šiame skirsnyje pabrėžiama, kad vyriausybės ir teisėsaugos institucijos gali piktnaudžiauti biometrinių duomenų rinkimu, ypač kai nėra aiškių teisinių pagrindų ir etinių gairių. Trečioji tema, pateikta 2.3 skirsnyje, yra Biometrikos instituto atliekama metinė pramonės apklausa. Šiame skyriuje pateikiamos įžvalgos apie tendencijas, bei iššūkius, su kuriais susiduria biometrinių duomenų pramonė, ypač privatumo, saugumo ir naudotojų pripažinimo klausimais. Ketvirtoji tema, pateikta 2.4. skirsnyje, apima „deepfake“ technologijos grėsmes biometrinėms sistemoms. Šiame skyriuje pateikiamos įžvalgos ir pastebėjimai, kaip technologija gali būti naudojama biometrinių sistemų atakoms, kaip apgavikai gali sukurti netikrus biometrinius duomenis, kurie gali būti naudojami kaip autentiški duomenys biometrinėje autentifikacijoje.

2.1. Šalių reitingavimas pagal biometrinių duomenų rinkimą ir panaudojimą

„Comparitech“ interneto svetainėje, kurioje pateikiami tyrimai ir yra viešinami didelio masto kibernetinio saugumo pažeidimai, įtakoję šimtus milijonų žmonių visame pasaulyje. Duomenų Tyrėjai Bond, C. ir Moody, R. (2022) pasidalino atliktu tyrimu „Kaip įmonės renka ir naudoja biometrinius duomenis“. Tyrimu siekta išsiaiškinti, kaip įmonės renka ir naudoja biometrinius duomenis, įskaitant, veido atpažinimo, pirštų atspaudų ir balso duomenis.

Metodologija: atlikdami tyrimą „Comparitech“ tyrėjai išanalizavo per 50 įvairių įmonių iš 100 pasaulio šalių, jų privatumo politiką ir paslaugų teikimo sąlygas, įskaitant pagrindines technologijų įmones, tokias kaip „Facebook“, „Google“ ir „Microsoft“, taip pat kitas įmones, kurios renka biometrinius duomenis įvairiais tikslais, pavyzdžiui, tapatybės patvirtinimo, prieigos kontrolės, ar stebėjimo tikslais. Autoriai analizavo įvairią prieinamą informaciją, įskaitant teisės aktus, naujienų straipsnius, pranešimus spaudoje ir vyriausybių skelbiamą informaciją. Tyrime taip pat nagrinėtos biometrinių duomenų rinkimo ir naudojimo teisinės sistemos įvairiose šalyse, įskaitant ES šalis, JAV, bei Aziją. Tyrime išskirtos aštuonios pagrindinės sritys, kurios buvo taikytos daugumai šalių, siekiant sąžiningai palyginti atskiras šalis ir užtikrinti duomenų prieinamumą. Sritys pagal kurias šalys buvo vertinamos, paskirstytos taip:

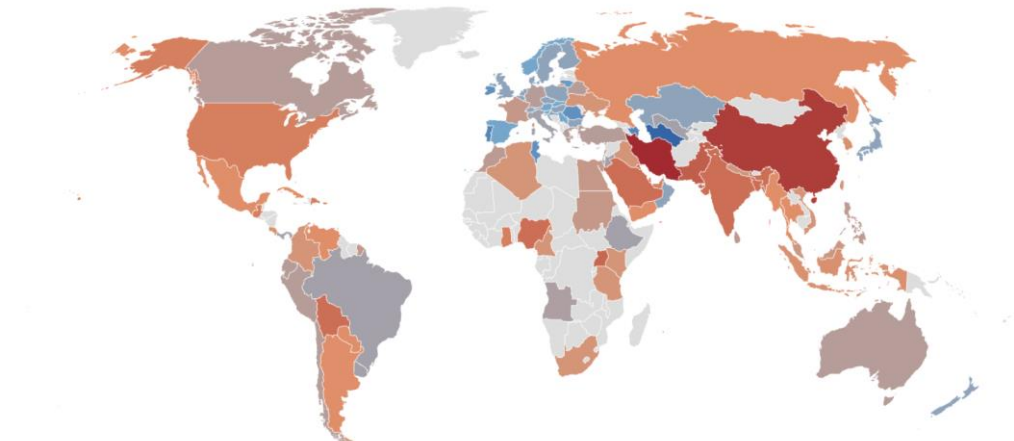
- Nacionaliniai pasai;

- Asmens tapatybės kortelė;
- Duomenų apsaugos įstatymas;
- Bankai;
- Rinkėjų registracija;
- Nacionalinė duomenų bazė;
- Policijos prieiga;
- Vaizdo stebėjimo kameros su veido atpažinimo funkcija;
- Darbo vieta;
- Vizų įvedimas;
- Biometriniai duomenys vizose;
- Biometriniai duomenys pasienyje.

Kiekviena šalis pagal pateiktas sritis, buvo vertinama 28 balų skalėje. Kuo balas žemesnis, tuo platesnis ir didesnis invazinis biometrinių duomenų naudojimo ir (arba) stebėjimo taikymas buvo nustatytas. Aukštesni balai reiškė, geresnius su biometrinių duomenų naudojimu ir stebėjimu susijusius apribojimus ir taisykles. Pagal pateiktas sritis buvo sudaryti penki klausimai, nusakantys biometrinių duomenų naudojimą specifinėje srityje ir esamą teisinį reguliavimą arba jo nebuvimą. Remiantis klausimynu ir sudaryta balų sistema, buvo sumodeliuotas šalių žemėlapis, atspindintis biometrinių duomenų rinkimo mastą (žr. 2 pav.).

Collection and storage of biometrics by country

Most Invasive Least Invasive



Šaltinis: Comparitech. (2021)

2 pav. Biometrinių duomenų rinkimo ir saugojimo pagal šalis žemėlapis

Iš šaltinyje pateikto paveikslėlio galima spręsti kiekvienos valstybės poziciją, dėl biometrinių duomenų rinkimo ir saugojimo. Paveikslėlyje pavaizduoti skirtingų šalių vertinimai, remiantis keliais kriterijais, didžiausia ir žemiausia invazija. Pagal šiuos kriterijus, galima įvertinti šalių požiūrį į

biometrinių duomenų rinkimą ir saugojimą. Šalys, kurių balai yra žemesni, parodė tendenciją rinkti didelius kiekius biometrinių duomenų ir / arba taikyti intensyvią stebėjimą ir priežiūrą. Tuo tarpu aukšti balai parodė, kad šalys yra geriau apsaugojusios piliečių biometrinius duomenis ir taiko griežtesnes taisykles ar apribojimus. Be to, paveikslėlyje galima pamatyti, kad kai kurios šalys turi lygius balus, kas reiškia, kad jų pozicija dėl biometrinių duomenų rinkimo ir saugojimo yra panaši.

Atradimai: tyrimo metu nustatyta, kad biometrinių duomenų rinkimas ir naudojimas įmonių tarpe yra plačiai paplitęs, beveik visos analizuotos įmonės renka vienokius ar kitokius biometrinius duomenis. Dažniausiai renkami biometriniai duomenys buvo veido atpažinimo duomenys, po jų sekė pirštų atspaudų ir balso duomenys. Tyrime taip pat nustatyta, kad dauguma įmonių biometrinius duomenis renka tapatybės patvirtinimo tikslais, tačiau kai kurios juos renka ir kitais tikslais, pavyzdžiui, personalizuotai reklamai ir stebėjimui vykdyti.

Tyrime nustatytos kai kurios nerimą keliančios biometrinių duomenų rinkimo ir naudojimo tendencijos. Pavyzdžiui, daugelis įmonių nepateikia aiškios informacijos apie tai, kaip jos renka ir naudoja biometrinius duomenis, todėl naudotojams siekiant priimti sprendimą, dėl sutikimo naudotis technologija, dažnai nėra viskas visiškai aišku, bei suprantama. Be to tyrimo metu nustatyta, kad kai kurios įmonės gali dalintis biometriniais duomenimis su trečiosiomis šalimis, arba naudoti juos stebėjimui ir be naudotojų žinios ar sutikimo. Tyrime taip pat nustatyta, kad biometrinių duomenų rinkimo ir naudojimo teisinės sistemos įvairiose šalyse stipriai skiriasi, o kai kuriose šalyse tėra tik kelios taisyklės apimančios asmens duomenų saugą, arba jų iš viso nėra taikoma.

Apribojimai: vienas iš vykdyto tyrimo apribojimų yra tas, kad buvo remtasi tik privatumo politikos ir paslaugų teikimo sąlygų analize, o tai galėjo netiksliai atspindėti, kaip įmonės iš tikrųjų renka ir naudoja biometrinius duomenis praktikoje. Taip pat tyrime nebuvo tiriamas biometrinių duomenų saugumas ir tai, kaip įmonės juos apsaugo nuo neteisėtos prieigos ar pažeidimų.

Išvados: iš atlikto tyrimo, galima spręsti, kad reikia griežtesnių biometrinių duomenų rinkimo ir naudojimo taisyklių. Daugiau skaidrumo, atskaitomybės iš tokius duomenis renkančių ir naudojančių įmonių. Vartotojams turėtų būti teikiama aiški informacija apie tai, kaip renkami ir naudojami jų biometriniai duomenys, jie turėtų turėti teisę atsisakyti tokių duomenų rinkimo ir naudojimo, tuo atveju kai toks noras yra. Tyrime taip pat pabrėžiama, kad svarbu imtis tinkamų priemonių biometriniais duomenims apsaugoti nuo neteisėtos prieigos ir pažeidimų.

2.2. Biometrinių duomenų ir elgsenos masinė stebėsena ES valstybėse narėse

Europos Parlamento Žaliųjų ir Europos laisvojo aljanso (Žaliųjų ir Europos laisvojo aljanso) frakcijos svetainėje, viešinamas autorių Ragazzi, F., Kuskonmaz, E. M., Plájás, I. Z., van de Ven, R., ir Wagner, B. (2021), atliktame tyrime „Biometrinių duomenų ir elgsenos masinė priežiūra ES valstybėse narėse“, pateiktoje tyrimo ataskaitoje, nagrinėjamas biometrinių stebėjimo technologijų

naudojimas ir paplitimas Europos Sąjungoje (ES). Tyrime atkreipiamas dėmesys į susirūpinimą keliančius klausimus, susijusius su biometrinių technologijų plėtra ir plačiu taikymu ES šalyse. Tyrime daugiausia dėmesio skiriama trims biometrinių stebėjimo technologijų rūšims: veido atpažinimui, eisenos atpažinimui ir emocijų atpažinimui. Tyrimu buvo siekiama iš probleminės pusės apžvelgti tai kas jau yra žinoma ir tai, kas šiuo metu vyksta ES šalyse, naudojant nuotolinį biometrinių identifikavimą, siekiant įvertinti, kokiais atvejais galima patekti į masinio biometrinio stebėjimo formas Greens/EFA Group in the European Parliament. (2021).

Metodologija: tyrime, siekiant išnagrinėti biometrinių stebėjimo technologijų naudojimą ES, naudojama literatūros apžvalga, teisinė analizė ir atvejų analizė. Tyrime analizuojamos šių technologijų reguliavimo sistemos skirtingose šalyse ir regionuose, pateikiama lyginamoji šių technologijų reguliavimo metodų analizė. Ataskaitoje taip pat remiamasi biometrinių stebėjimo technologijų naudojimo ES atvejų tyrimais, siekiant atkreipti dėmesį į su jų diegimu susijusią riziką ir keliamus iššūkius.

Atradimai: tyrime nustatyta, kad biometrinių stebėjimo technologijų naudojimas ES sparčiai didėja, o vyriausybės ir teisėsaugos institucijos diegia šias technologijas įvairiais tikslais, įskaitant sienų kontrolę, visuomenės saugumą ir nusikaltimų prevenciją. Tyrime nustatyta keletas susirūpinimą keliančių aspektų, susijusių su šių technologijų diegimu, įskaitant tai, kad jos gali pažeisti pagrindines teises ir laisves, pavyzdžiui, privatumą ar duomenų apsaugą. Tyrime taip pat atkreiptas dėmesys į šališkumo ir klaidų riziką šiose technologijose, į iššūkius, susijusius su demokratinės priežiūros, bei atskaitomybės užtikrinimu diegiant šias technologijas.

Tyrime nustatyta, kad biometrinių stebėjimo technologijų reguliavimo sistemos įvairiose šalyse ir regionuose labai skiriasi, o kai kuriose šalyse teisinės sistemos yra tvirtesnės nei kitose. Tyrime teigiama, kad šių technologijų diegimui turėtų būti taikomos tinkamos apsaugos priemonės, bei priežiūros mechanizmai, kad būtų apsaugotos pagrindinės teisės ir laisvės. Tyrime išskirtinos septynios rekomendacijos ES šalims Greens/EFA Group in the European Parliament. (2021):

1. ES turėtų uždrausti viešosiose erdvėse diegti tiek masinio, tiek tikslinio nuotolinio biometrinio ir elgsenos identifikavimo (RBI) technologijas (RBI realiuoju laiku), taip pat identifikavimo (arba teismo ekspertizės RBI). Tyrime autorių atlikta analizė parodė, kad abi šios praktikos, net jei jos naudojamos „tiksliniam stebėjimui“ yra prilyginamos masiniam stebėjimui.

2. ES turėtų sustiprinti biometrinių ir elgsenos atpažinimo technologijų skaidrumą ir atskaitomybę.

3. ES turėtų skatinti stiprinti patikimus biometrinių stebėjimo sistemų atskaitomybės mechanizmus.

4. ES turėtų skatinti asmens teisių užtikrinimą pagal Bendrąjį duomenų apsaugos reglamentą (BDAR).

5. ES turėtų užtikrinti veiksmingą BDAR tikslų ir apribojimų vykdymo užtikrinimą.

6. ES turėtų remti organizacijas, kurios mobilizuoja už pagarbą ES pagrindinėms teisėms.

7. ES turėtų atsižvelgti į pasaulinį biometrinių ir elgesio analizės technologijų pramonės aspektą.

Apribojimai: vienas iš tyrimo apribojimų yra tas, kad jame daugiausia dėmesio skiriama biometrinių stebėjimo technologijų naudojimui ES, todėl tai pilnai neatspindi padėties kituose regionuose ar šalyse. Tyrime taip pat ribotai aptariama galima biometrinio stebėjimo technologijų nauda, kuri galėtų būti labiau subalansuota iš technologijų poveikio analizės.

Išvados: iš atlikto tyrimo galima spręsti, kad biometrinių stebėjimo technologijų diegimas turėtų būti pagrįstas aiškiu ir įtikinamu viešuoju interesu ir jam turėtų būti taikoma demokratinė priežiūra ir atskaitomybė. Tyrime politikos formuotojams rekomenduojama laikytis atsargumo principo diegiant šias technologijas ir užtikrinti, kad jų naudojimui būtų taikomos tinkamos apsaugos priemonės ir priežiūros mechanizmai. Tyrime taip pat raginama sukurti tvirtą ES reguliavimo sistemą, kuri reglamentuotų biometrinių stebėjimo technologijų diegimą, ypač daug dėmesio skiriant pagrindinių teisių ir laisvių apsaugos užtikrinimui.

2.3. Biometrikos instituto metinė pramonės apklausa

Biometrikos institutas nuo 2010 metų, kas metus kviečia pramonės profesionalus iš viso pasaulio dalyvauti, organizuojamoje kasmetinėje apklausoje. Kurios tikslas pateikti įžvalgų apie dabartinę biometrijos pramonės būklę, ateities kryptis, taip pat apie iššūkius, galimybes, įtakančias technologijų augimą ir plėtrą. 2019 metais vykdytoje apklausoje, dalyvavo Biometrikos instituto nariai, bei kitos suinteresuotos šalys visame pasaulyje, o atsakymus pateikė per 453 asmenų iš viešojo ir privataus sektoriaus, mažiau nei pusė (45 %) pateiktų atsakymų sudarė Biometrijos instituto nariai Biometrics Institute. (2019). Vykdytoje apklausoje pateikiama išsami rezultatų analizė, suskirstyta į įvairias temas ir potemes. Pradžioje apžvelgiamos pagrindinės apklausos išvados, pabrėžiama, kad biometriniai duomenys vis plačiau diegiami įvairiuose sektoriuose, taip pat su jų naudojimu susiję iššūkiai ir pavojai. Toliau ataskaitoje gilinamasi į konkrečias temas, pavyzdžiui, veido atpažinimo naudojimą ir „COVID-19“ pandemijos poveikį biometrijos pramonei.

Metodologija: apklausos metu buvo renkami kiekybiniai ir kokybiniai duomenys apie biometrinių technologijų naudojimą įvairiuose sektoriuose.

Atradimai: ataskaita atskleidė, kad biometrinių technologijų diegimas stipriai plečiasi: 96 % respondentų nurodė, kad jų organizacija naudoja arba planuoja naudoti biometrines technologijas. Biometrinių technologijų tipai, kaip pirštų atspaudų atpažinimas išliko plačiausiai naudojama biometrinė technologija, po kurios seka veido ir akies rainelės atpažinimas. Nustatytas padidėjęs balso atpažinimo ir elgsenos biometrinių duomenų naudojimo atvejų kiekis. Ataskaitoje akcentuoti biometrinių technologijų diegimo iššūkiai, įskaitant išlaidas, techninius klausimus ir susirūpinimą dėl privatumo, bei duomenų apsaugos. Visuomenės požiūris į biometrines technologijas išliko

nevienareikšmis, o dažniausiai reiškiamas susirūpinimas, dėl privatumo ir saugumo, sprendžiant iš ataskaitoje pateikiamų rezultatų. Dauguma respondentų pritarė, kad norint veiksmingai ir etiškai naudoti biometrines technologijas, būtina nustatyti standartus ir reglamentavimą. Taip pat nurodė, kad didžiausias rūpestis kyla, dėl privatumo, duomenų apsaugos ir kibernetinių grėsmių rizikos. Apklausą taip pat atskleidė, kad daugeliui organizacijų trūksta reikiamų įgūdžių, žinių, siekiant veiksmingai įgyvendinti biometrinius sprendimus, laikytis atitinkamų reglamentų ir įstatymų.

Didelę reikšmę buvo skirta ir „COVID-19“ poveikio įtakai biometrijos pramonei analizavime. Kaip parodė apklausos duomenys, pandemija paspartino neliečiamosios biometrijos ir nuotolinio tapatybės tikrinimo sprendimų diegimą ir taikymą, organizacijoms siekiant sumažinti fizinio kontakto būtinybę, bei saugaus socialinio atstumo užtikrinimui. Pandemija taip pat išryškino būtinybę taikyti griežtą duomenų apsaugos ir privatumo politiką, kad būtų užkirstas kelias netinkamam biometrinių duomenų naudojimui ar piktnaudžiavimui.

Išvados: atliktas tyrimas parodė, kad biometrijos pramonė turi didelį augimo ir plėtros potencialą, tačiau šis augimas turi būti derinamas su atsakingu ir etišku biometrinių technologijų naudojimu. Apklausos rezultatai parodė, kad daugeliui organizacijų svarbiausi yra privatumo ir duomenų apsaugos klausimai. Taip pat, kad reikia daugiau įgūdžių ir žinių, siekiant veiksmingai įgyvendinti biometrinius sprendimus, laikantis atitinkamų reglamentų, ar įstatymų. Ateityje pramonė turi toliau diegti naujoves, kurti naujus biometrinius sprendimus, kurie suderintų saugumą su privatumu ir duomenų apsauga, užtikrintų priimtina patogumo lygį, taip pat atsižvelgti į kintančius įvairių sektorių, bei pramonės šakų poreikius bei iššūkius.

2.4. Deepfake technologijos grėsmės biometrinėms sistemoms

Saugios biometrinių tapatybių patvirtinimo sprendimų įmonės „iProov“, 2021 m. atliktas tyrimas, pavadinimu „Deepfakes: Is This the End of Trust?“ išnagrinėjo „deepfake“ technologijos panaudojimą biometrinių sistemų atakoms vykdyti, sukuriant netikrus biometrinius duomenis. Tyrimo metu buvo ištestuota, ar technologiją galima panaudoti tam, kad apgauti veido ir balsų atpažinimo sistemas. Tyrimo tikslas buvo ištirti „deepfake“ technologijos poveikį biometrinėms sprendimams, ir nustatyti, kaip ši technologija gali paveikti saugumą ir patikimumą. Tyrimo struktūra buvo parengta taip, kad būtų galima apimti kuo daugiau skirtingų aspektų, susijusių su šia technologija, taip pat pateikti rekomendacijas, kaip išvengti galimų problemų.

Metodologija: tyrimas pradėtas nuo literatūros apžvalgos, siekiant geriau suprasti „deepfake“ technologiją ir jos potencialą biometrinių sistemų atakoms. Po to buvo atlikti eksperimentai, kurie apėmė „deepfake“ vaizdo medžiagos sukūrimą ir bandymą autentifikuoti save naudojant suklaidotus vaizdo įrašus. Eksperimentų metu, tyrėjai sukūrė „deepfake“ vaizdo įrašus naudodamiesi trimis skirtingais „deepfake“ įrankiais: „DeepFaceLab“, „Faceswap“ ir „NeuralTextures“. Tyrimui atlikti

panaudoti viešai prieinami vaizdų ir garso įrašų duomenų rinkiniai. Sukurti „deepfake“ vaizdo įrašai buvo bandyti autentifikuoti naudojant „iProov“ biometrinę autentifikacijos sistemą. Buvo matuojamas „deepfake“ vaizdo įrašų autentifikavimo tikslumas, t.y. kiek procentų atvejų, sistemos autentifikavo vaizdo įrašą kaip tikrąjį.

Atradimai: tyrimo metu buvo nustatyta, kad „deepfake“ technologijos kelia didelę grėsmę biometrinėms sistemoms. Tyrimo autoriai parodė, kad technologija gali būti naudojama siekiant apgauti biometrines sistemas, kurios naudoja vaizdo arba garso atpažinimą. Taip pat nustatyta, kad ši technologija yra ne tik lengvai prieinama, bet ir gali būti naudojama nežinomų asmenų, kurie neturi aukšto technologinio išsilavinimo. Tyrimo metu buvo nustatyta, kad „deepfake“ technologiją yra itin sudėtinga aptikti. Autoriai išbandė kelias biometrines sistemas, kurios naudoja vaizdo arba garso atpažinimą, ir nustatė, kad net patikimiausios sistemos gali būti lengvai apgautos pasitelkiant šią technologiją. Tyrimo autoriai taip pat pabrėžė, kad „deepfake“ technologija gali būti naudojama ne tik atakų prieš biometrines sistemas metu, bet ir toliau, siekiant manipuluoti informacija internete. Ši technologija gali būti naudojama siekiant sukurti netikrus naujienų pranešimus, politinius skandalus, sukčiavimus ir kitus potencialius nusikaltimus.

Galiausiai, tyrimo metu buvo pateiktos rekomendacijos, kaip galima apsisaugoti nuo „deepfake“ technologijos poveikio biometrinėms sistemoms. Autoriai rekomendavo naudoti patikimas biometrines sistemas, kurios naudoja kelis autentifikavimo veiksnius, kad būtų sudarytos sąlygos daugialypei autentifikacijai. Taip pat rekomendavo naudoti saugius ryšio kanalus, kad būtų užtikrinta duomenų perdavimo sauga.

Išvados: atliktas tyrimas parodė, kad „deepfake“ technologija yra didelė grėsmė biometrinėms sistemoms, asmens privatumui ir duomenų apsaugai. Technologijos naudojimas suteikia pagalbą lengvai be didesnių technologinių žinių vykdyti biometrinių sistemų atakas. Nustatyta, jog siekiant apsaugoti biometrines sistemas nuo galimų atakų, reikia naudoti patikimas autentifikavimo priemonės ir stebėti, ar naudojamos biometrinės sistemos yra atsparios naujoms potencialioms atakoms. Galimos ateities biometrinės sistemos turi būti kuriamos taip, kad būtų atsparios naujoms ir kylančioms atakų rūšims, įskaitant „deepfake“ technologiją. Reikalingas glaustas bendradarbiavimas tarp privataus ir viešojo sektorių, siekiant kurti efektyvesnes priemones biometrinių atakų prevencijai.

3. LIETUVOS VARTOTOJŲ POŽIŪRIO Į BIOMETRINES TECHNOLOGIJAS IR ASMENS DUOMENŲ SAUGUMĄ TYRIMO METODOLOGIJA

Šiame skyriuje pateikiama tyrimo metodika, siekiant išsiaiškinti Lietuvos vartotojų požiūrį į biometrines technologijas ir asmens duomenų saugumą. Pirmame skyriuje apibrėžiama tyrimo metodika, pateikiamas tyrimo tikslas ir objektas, tyrimui keliami uždaviniai, tyrimo vykdymo etapai. Antrame skyriuje pateikiama ekspertinio interviu vykdymo metodika, kurioje detalizuojama tyrimo imtis, ekspertų atranka, ekspertų charakteristikos, pateikiami ekspertinės apklausos anketos klausimai ir išsikelti tikslai.

3.1. Tyrimo metodika

Tyrimas atliktas taikant mišrių metodų metodiką, kuri apjungė kokybinių ir kiekybinių duomenų rinkimą ir analizę. Toks metodas yra naudingas, nes jis leidžia gauti platesnį vaizdą apie tyrimo temą, taip pat gilintis į klausimus iš kelių skirtingų perspektyvų. Kiekybiniai duomenys suteikia galimybę suskaičiuoti tam tikrus rodiklius ir gauti statistiką, tuo tarpu kokybiniai duomenys suteikia galimybę giliau išnagrinėti respondentų požiūrį ir patirtis. Kaip teigia Leedy ir Ormrod (2020), toks mišrus metodas leidžia gauti tikslesnį ir pilnesnį vaizdą apie tyrimo objektą, todėl yra naudingas ir efektyvus.

Tyrimo tikslas – ištirti Lietuvos vartotojų požiūrį į biometrines technologijas ir jų įtaką asmens duomenų saugumui, siekiant suformuoti rekomendacijas, kaip padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje.

Tyrimo objektas – biometrinės technologijos ir jų poveikis asmens duomenų apsaugai.

Tyrimo uždaviniai:

1. Įvertinti esamą biometrinių technologijų situaciją Lietuvoje ir nustatyti pagrindines tendencijas ir iššūkius, kuriuos ši sritis patiria.
2. Išnagrinėti galimą biometrinių technologijų keliamą riziką ir iššūkius asmens duomenų saugumui.
3. Įvertinti visuomenės susipažinimą su Lietuvos, ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą ir apsaugą.
4. Ištirti visuomenės požiūrį ir suvokimą apie biometrinių technologijų naudojimą asmens duomenims rinkti ir tvarkyti.
5. Pasiūlyti rekomendacijas ir sprendimus, kaip šalinti biometrinių technologijų keliamas grėsmes asmens duomenų apsaugai.

Tyrimo etapai ir procesas:

Literatūros apžvalga: pirmajame etape buvo atlikta atitinkamos literatūros ir dokumentų, susijusių su biometrinėmis technologijomis ir asmens duomenų apsauga, apžvalga. Tai apėmė mokslinius straipsnius, knygas, ataskaitas ir vyriausybinius teisės aktus.

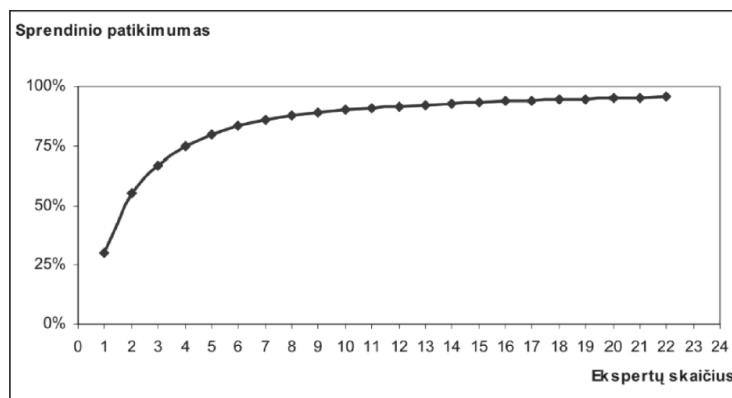
Kokybinių duomenų rinkimas: antrajame etape buvo renkami kokybiniai duomenys, atliekant pusiau struktūruotus interviu su informacinių technologijų ir asmens duomenų apsaugos srities ekspertais. Interviu buvo atliekami naudojant iš anksto parengtą klausimų rinkinį. Orientuojantis į ekspertų turimą patirtį ir požiūrį, į biometrinių technologijų naudojimo sąlygojamas grėsmes, bei galimas rizikas.

Kiekybinių duomenų rinkimas: trečiajame etape kiekybiniai duomenys buvo renkami atliekant internetinę suaugusių Lietuvos gyventojų apklausą. Apklausą sudarė 24 klausimai, siekiant ištirti dalyvių požiūrį į biometrinių technologijų naudojimą ir tinkamą asmens duomenų apsaugos užtikrinimą.

Duomenų analizė: ketvirtajame etape buvo analizuojami ankstesniais etapais surinkti kokybiniai ir kiekybiniai duomenys. Kokybiniai duomenys buvo analizuojami teminiu būdu, nustatant interviu metu išryškėjusius modelius ir temas. Kiekybiniai duomenys buvo analizuojami naudojant aprašomąją statistiką.

3.2. Ekspertų interviu

Tyrimo imtis ir ekspertų atranka. Tyrimui atlikti buvo taikoma tikslinė ekspertų atranka, ekspertai buvo atrinkti pagal tam tikrus kriterijus, susijusius su darbo sritimi, ne mažesnę nei 10 metų darbo stažą, turimomis žiniomis, bei patirtimi, informacinių technologijų ir asmens duomenų saugumo srityje. Kaip teigia Leedy ir Ormrod (2020), tikslinė atranka yra tinkama, kai tyrėjas siekia identifikuoti tam tikrus atvejus ir atlikti giluminę analizę, o ne tik apibendrintą populiacijos vaizdą. Siekiant optimizuoti tyrimo laiką ir turimus išteklius, pasirinktas nedidelio dydžio 5 ekspertų grupės apklausos metodas. Remiantis moksliniais tyrimais, šios grupės dydis gali būti nuo 3 iki 7 narių (žr. 3 pav.) Augustinaitis, Rudzkienė, Petrauskas ir kt. (2009).

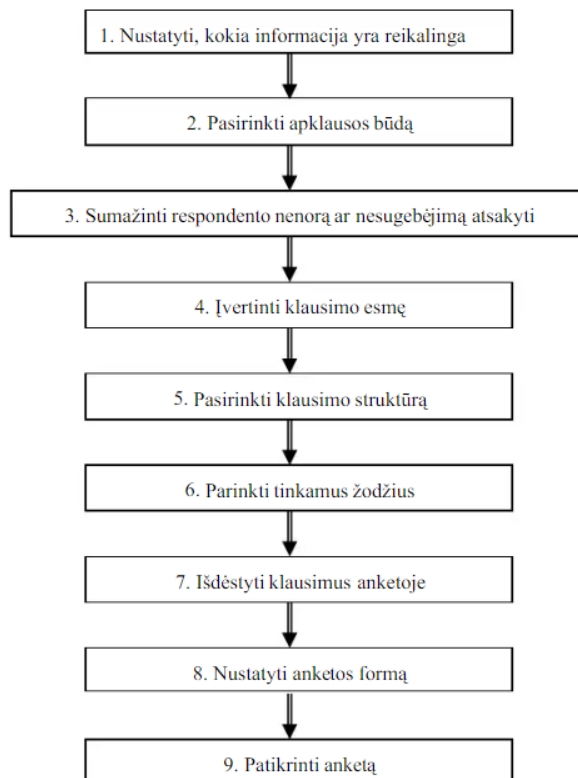


Šaltinis: Augustinaitis, Rudzkienė, Petrauskas ir kt. (2009)

3 pav. Ekspertų grupės dydžio poveikis patikimumui

Iš šaltinyje pateikto paveikslėlio galima spręsti, kad tokios ekspertų grupės skaičius, rezultatų patikimumo prasme sieks apie 80 %. Todėl, šiuo atveju nustatant 5 ekspertų skaičiaus tikslinę grupę, vykdant apklausą, galima tikėtis gauti reikšmingų ir tikslių tyrimo rezultatų, kuriuos galima panaudoti sprendimų priėmimo procese.

Ekspertų charakteristikos. Ekspertai buvo pasirinkti iš įvairių organizacijų, įskaitant viešąsias, privačias įmones, akademinę bendruomenę ir viešąjį sektorių. Ekspertai buvo atrenkami orientuojantis į konkretų tikslą, siekiant sužinoti esamą nuomonę ir turimą patirtį, gauti rekomendacijas, dėl biometrinių technologijų naudojimo Lietuvoje, užtikrinant asmens duomenų saugumą ir privatumą. Siekiant padidinti galimybes įvykdyti sėkmingą ekspertų apklausą ir surinkti nuomones, bei pasiūlymus, taikytas anoniminės apklausos metodas. Visi apklausti ekspertai buvo informuoti apie savo teises ir galimybes dalyvaujant tyrimo metu, taip pat apie jų atsakymų anonimiškumo užtikrinimą. Ekspertams priskirti identifikavimo kodai (E1, E2, E3, E4 ir E5). Ekspertų atsakymams gauti, panaudotas kokybinės apklausos metodas, sudarant klausimų anketa pagal Vytautą Dikčią (2011) (žr. 4 pav.)



Šaltinis: Vytautas Dikčias (2011)

4 pav. Ekspertų anketos sudarymo nuoseklumas

Apklausa buvo sudaryta iš 10 atviro tipo klausimų, kurioje klausiama ekspertų nuomonės apie biometrinių technologijų naudojimą, įtaką asmens duomenų saugumui Lietuvoje ir galimas rekomendacijas. Sudarant anketa, pirminiame etape, buvo nustatyta, kokios informacijos ir kokių rekomendacijų sėkmingam tyrimo vykdymui iš ekspertų tikimasi sulaukti. Remiantis autoriumi

Vytautu Dikčiumi (2011), pakankamai svarbu tinkamai suprasti kas bus tiksliniai apklausos dalyviai, kadangi priklausomai nuo tikslinės auditorijos, reikalingas atitinkamas žodžių ir klausimyno parinkimas. Antrame etape buvo parenkamas apklausos būdo tipo nustatymas. Kadangi apklausai vykdyti buvo pasirinkta tikslinė ekspertų grupė, sudaryti aiškūs ir suprantami apklausos dalyviams orientuoti klausimai. Trečiajame etape įvertinta sudarytų klausimų esmė, siekiant nenukrypti nuo siekiamo tikslo. Klausimai sudaryti taip, kad surinkta informacija būtų svarbi vykdomo tyrimo tikslui pasiekti.

Apklausos anketos klausimai ir tikslai:

1. Kokią įtaką, jūsų nuomone, biometrinės technologijos daro asmens duomenų saugumui Lietuvoje ir kokia galima šių technologijų rizika ir nauda?

Klausimo tikslas – įvertinti biometrinių technologijų įtaką asmens duomenų saugumui Lietuvoje ir išnagrinėti galimas rizikas ir naudą, kurią šios technologijos gali teikti.

2. Kokios yra aktualiausios etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims rinkti ir tvarkyti, kaip šias problemas galima būtų spręsti?

Klausimo tikslas – aptarti aktualiausias etines problemas, susijusias su biometrinių technologijų naudojimu asmens duomenims rinkti ir tvarkyti, bei pasiūlyti galimas sprendimo strategijas šioms problemoms spręsti.

3. Kaip vertinate dabartinę biometrinių technologijų situaciją Lietuvoje, kokias pagrindines tendencijas ir iššūkius matote šioje srityje?

Klausimo tikslas – apibūdinti dabartinę biometrinių technologijų situaciją Lietuvoje, išskirti pagrindines tendencijas ir iššūkius šioje srityje.

4. Kokios teisinės ir reguliavimo sistemos šiuo metu Lietuvoje reglamentuoja biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui, kaip manote, kiek veiksmingai šios sistemos apsaugo asmens privatumo teises?

Klausimo tikslas – išnagrinėti teisines ir reguliavimo sistemas, kurios reglamentuoja biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui Lietuvoje, įvertinti šių sistemų veiksmingumą asmens privatumo teisių apsaugos atžvilgiu.

5. Kaip manote, koks vaidmuo gali tekti vartotojų švietimui ir informuotumo didinimo kampanijoms, siekiant informuoti Lietuvos visuomenę apie biometrinių technologijų tinkamą naudojimą, bei sąlygojamas grėsmes, ir kokios strategijos šiuo atžvilgiu būtų veiksmingiausios?

Klausimo tikslas – apsvarstyti vartotojų švietimo ir informuotumo didinimo kampanijų svarbą, siekiant informuoti Lietuvos visuomenę apie biometrinių technologijų tinkamą naudojimą, sąlygojamas grėsmes, bei pasiūlyti veiksmingas strategijas šiuo atžvilgiu.

6. Kaip biometrinės technologijos galėtų būti kuriamos ir diegiamos, siekiant užtikrinti didesnę privatumo, bei saugumo lygį, tuo pačiu teikiant naudą vartotojams ir organizacijoms?

Klausimo tikslas – aptarti galimus būdus, kaip biometrinės technologijos gali būti kuriamos ir diegiamos, siekiant užtikrinti didesnę privatumo ir saugumo lygį, tuo pačiu teikiant naudą vartotojams ir organizacijoms.

7. Kaip būtų galima atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus, kad būtų galima spręsti unikalios biometrinių technologijų keliamus iššūkius ir kokie vykdymo užtikrinimo mechanizmai būtų veiksmingiausi šiame kontekste?

Klausimo tikslas – pasiūlyti galimus būdus, kaip galima būtų atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus, siekiant spręsti unikalios biometrinių technologijų keliamus iššūkius, ir įvertinti, kokie vykdymo užtikrinimo mechanizmai būtų veiksmingiausi šioje srityje.

8. Kokį vaidmenį, jūsų nuomone, atlieka pramonės savireguliacija skatinant atsakingą biometrinių technologijų naudojimą ir kokios yra pagrindinės veiksmingos savireguliacijos sistemos sudedamosios dalys?

Klausimo tikslas – išsiaiškinti pramonės savireguliacijos vaidmenį ir veiksmingas savireguliacijos sistemos sudedamąsias dalis biometrinių technologijų naudojimo atsakingumui didinti.

9. Kaip, jūsų nuomone, biometrinių technologijų naudojimas Lietuvoje vystysis artimiausiais metais ir kokį poveikį tai turės asmens duomenų saugumo ir privatumo užtikrinimui?

Klausimo tikslas – prognozuoti biometrinių technologijų vystymosi perspektyvas Lietuvoje ir įvertinti jų poveikį asmens duomenų saugumui ir privatumui.

10. Kokias pasiūlytumėte pagrindines rekomendacijas ar sprendimus, siekiant padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje ir kaip šios rekomendacijos galėtų būti įgyvendintos praktiškai?

Klausimo tikslas – pasiūlyti pagrindines rekomendacijas ar sprendimus, kurių įgyvendinimas padėtų padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje, ir apibūdinti galimas praktines šių rekomendacijų įgyvendinimo priemones.

4. LIETUVOS VARTOTOJŲ POŽIŪRIO Į BIOMETRINES TECHNOLOGIJAS IR ASMENS DUOMENŲ SAUGUMĄ EMPIRINIO TYRIMO REZULTATAI

Šiame skyriuje atskleidžiamas Lietuvos vartotojų požiūris į biometrines technologijas ir asmens duomenų saugumą. Pateikiamos ekspertų įžvalgos ir nuomonė apie biometrinių technologijų naudojimą ir poveikį asmens duomenų saugumui. Skyrių sudaro septynios temos perteikiančios tyrimo metu gautus rezultatus. Pirmosios penkios temos apima ekspertų interviu metu surinktos informacijos rezultatų detalizavimą ir išvadas. Šeštoji tema skirta atskleisti Lietuvos vartotojų nuomonę ir požiūrį į biometrines technologijas. Septintoji paskutinė tema apima tyrimo metu gautų rezultatų pritaikymą ruošiant biometrinių technologijų plėtros atsparumo grėsmėms modelį.

4.1. Biometrinių technologijų įtaka asmens duomenų saugumui ir privatumui

Biometrinės technologijų įtaka asmens duomenų saugumui Lietuvoje, galima šių technologijų rizika ir nauda. E1 ekspertas pasisakydamas apie situaciją Lietuvoje, pabrėžė, jog biometrinės technologijos gali turėti tiek teigiamų, tiek neigiamų poveikių asmens duomenų saugumui. Anot eksperto, įgyvendinus biometrinių technologijų taikymą, galima padidinti asmens duomenų saugumą ir apsaugoti juos nuo galimų nusikalstamų veiksmų, tokiose srityse kaip bankininkystė, verslo valdymas ir t.t. Tačiau, biometrinių technologijų naudojimas anot eksperto, taip pat kelia riziką asmens duomenų privatumui, nes šie duomenys yra ypatingai jautrūs ir gali būti naudojami nelegaliai arba netinkamai. Eksperto nuomone svarbu, kad biometrinės technologijos būtų naudojamos atsakingai ir pagal gerąją praktiką, kad būtų užtikrintas asmens duomenų saugumas, bei privatumas. Be to, svarbu, kad reguliavimo ir priežiūros mechanizmai būtų stiprinami nuolatos, siekiant užtikrinti tinkamą biometrinių duomenų naudojimą ir saugumą. Kaip galimas biometrinių technologijų rizikas ekspertas išskiria:

- nelegalus biometrinių duomenų rinkimas;
- netinkamas duomenų tvarkymas;
- asmens duomenų nutekėjimas;
- diskriminacija.

Todėl eksperto nuomone svarbu, kad biometrinės technologijos būtų naudojamos atsargiai ir su tinkamais reguliavimo ir priežiūros mechanizmais, kad būtų užtikrintas asmens duomenų saugumas ir privatumas.

E2 eksperto nuomone biometrinės technologijos, kaip ir bet kurios kitos technologijos naudojamos geram tikslui visokeriopai yra naudingos. Anot eksperto šių technologijų kaip ir, bet kurių kitų technologijų naudojimo rizikas sukelia pats žmogus, norėdamas jas naudoti savanaudiškai, ar

piktiems kėslams. Todėl reikalingi susitarimai, baudos, taisyklės. Tačiau žmogus nėra robotas ir vis tiek jas pažeidinės.

E3 ekspertas teigė, kad viskas stipriai priklauso nuo to koks bus sukurtas teisinis reguliavimas ir kokie saugumo reikalavimai bus taikomi duomenų centrams kurie saugos šiuos duomenys. Pagrindines naudas ekspertas įžvelgė įvairiems analizės centrams, privačioms pelno siekiančios kompanijoms.

E4 eksperto nuomone biometrinių technologijų taikymas suteiks galimybes pasiekti aukštesnį saugumo lygį, dėl savo unikalumo ir klastojimo sudėtingumo. Kaip galimas rizikas ekspertas išskyrė susijusias su poreikiu diegti papildomas technines priemones biometrinių duomenų nuskaitymui.

E5 eksperto nuomone biometrinių technologijų naudojimas suteiks lengvesnį duomenų panaudojimą, analizės galimybes. Kaip galima rizikas ekspertas išskyrė, duomenų nutekėjimą ir biometrinių duomenų nutekėjimą į netinkamas rankas.

Išvados: atsižvelgiant į ekspertų išsakytą nuomonę, galima daryti išvadas, kad biometrinės technologijos turi potencialą padidinti asmens duomenų saugumą ir apsaugoti vartotojus nuo galimų nusikalstamų veiksmų, tačiau šių technologijų naudojimas taip pat kelia tam tikras rizikas asmens duomenų privatumui. Labai svarbu tinkamas biometrinių technologijų naudojimas, tinkamas reguliavimų ir priežiūros mechanizmų taikymas.

Biometrinių technologijų kūrimas ir diegiamas, siekiant užtikrinti didesnę privatumo ir saugumo lygį, tuo pačiu teikiant naudą vartotojams ir organizacijoms.

E1 eksperto nuomone biometrinių technologijų kūrimas, bei diegimas turėtų būti atliekamas atsakingai, remiantis principais, kurie užtikrintų asmens duomenų saugumą ir privatumą. Ekspertas teigia, jog tam, kad būtų užtikrintas didesnis privatumo ir saugumo lygis, biometrinių technologijų kūrėjai, bei diegėjai turėtų atlikti šiuos veiksmus:

- atsižvelgti į duomenų apsaugos principus ir privatumo principus, nustatytus teisės aktuose;
- įdiegti saugumo protokolus ir technologijas, kurios užtikrintų, kad asmens duomenys yra saugūs;
- užtikrinti, kad duomenys yra anonimiški arba neidentifikuojami, jei tai yra įmanoma;
- suteikti vartotojams galimybę kontroliuoti savo duomenis ir nustatyti savo privatumo nustatymus;
- vykdyti tyrimus, ar testavimus, siekiant įvertinti biometrinių technologijų veikimo efektyvumą ir patikimumą.
- bendradarbiauti su duomenų apsaugos institucijomis ir kitais susijusiais subjektais, siekiant užtikrinti, jog biometrinės technologijos atitiktų teisės aktus ir būtų saugios vartotojams.

E2 eksperto nuomone, visų pirma biometrinės technologijos turėtų būti kuriamos iš saugumo, bet ne iš funkcionalumo perspektyvos. Tačiau tai reikalauja didesnių investicijų, kas ne visada paranku konkurencinėje kovoje. Tuo pačiu visiškai užtikrinti biometrinių duomenų saugumą, kaip ir bet kokių

duomenų saugumą yra neįmanoma. Eksperto manymu biometriniai duomenys gali būti panaudojami tik kaip papildantieji duomenys.

E3 ekspertas teigė, jog techninė ir programinė įranga, renkanti, apdorojanti, bei sauganti biometrinius duomenis turi atitikti aukščiausius saugumo reikalavimus. Turi būti įdiegti atitinkami kontrolės mechanizmai. Vartotojų patogumui pasiekti, šios priemonės turi būti taikomos su minimaliu vartotojo įsikišimu.

E4 ekspertas pabrėžė, kad yra būtinas aiškus teisinis reglamentavimas. Saugumo procesų valdymas kūrimo ir diegimo yra pirminis poreikis bei būtinybė.

E5 ekspertas teigė šiuo metu neįsivaizduojantis koks tai turėtų būti procesas siekiant užtikrinti didesnę privatumo ir saugumo lygį.

Išvados: iš visų ekspertų atsakymų galima daryti išvadas, kad yra būtinas atsakingas biometrinių technologijų naudojimas, atsižvelgiant į duomenų apsaugos ir privatumo principus. Siekiant padidinti ir užtikrinti didesnę privatumo, bei saugumo lygį būtinos papildomos investicijos. Svarbu, kad techninė ir programinė įranga, atitiktų aukščiausius saugumo reikalavimus, būtų diegiami atitinkami kontrolės mechanizmai. Biometriniai duomenys turėtų būti naudojami kaip papildantieji duomenys, jei tik tai yra įmanoma. Svarbus bendradarbiavimo vaidmuo su duomenų apsaugos institucijomis ir kitais susijusiais subjektais. Yra būtinas aiškus teisinis reglamentavimas, užtikrinantis tinkamą saugumo procesų valdymą, kūrimą ir diegimą. Tinkamas technologijų adaptavimas atsižvelgti į vartotojų patogumą.

Pagrindinės rekomendacijos, sprendimai, siekiant padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje ir rekomendacijų įgyvendinimas praktiškai.

E1 ekspertas rekomenduojo, kad Lietuvoje būtų įvesti aiškūs ir griežti teisės aktai, reglamentuojantys biometrinių technologijų naudojimą ir asmens duomenų apsaugą. Būtų svarbu užtikrinti, kad visi subjektai, kurie tvarko asmens duomenis, laikytųsi šių taisyklių ir taikytų saugumo priemones, kad būtų užtikrintas privatumas ir saugumas. Ekspertas taip pat pabrėžė, jog taip pat reikia skatinti vartotojų švietimą ir informavimą apie biometrinių technologijų naudojimą ir susijusias rizikas, kad jie galėtų priimti informuotus sprendimus ir apsaugoti savo privatumą. Taip pat būtų svarbu skatinti organizacijas naudoti tik patikrintas ir saugias biometrines technologijas, bei vykdyti reguliarias duomenų saugumo patikras ir atnaujinimus.

E2 ekspertas mano, kad iš esmės sprendimai šioje srityje, tikėtina kad bus sprendžiami tik Europos sąjungos kontekste, bet ne individualiai Lietuvos kontekste. Tačiau eksperto nuomone, Lietuva gali inicijuoti biometrinių duomenų apibrėžimo ir naudojimo platesnį EU reglamentavimą. Tačiau tokių technologijų reglamentavimas turėtų būti savalaikiškas (t.y. pakeitimus turėtų būti galima atlikti greitai). Tai ir reikštų praktinį problemos sprendimą - EU teisės pritaikymą, bei greitą reakciją į besikeičiančias technologines realijas. Lietuvos kontekste individualūs sprendimai gali būti per

brangūs ir neapsimokėti. Kita vertus, biometrinių duomenų pertekliniai apribojimai stabdys technologijų plėtrą ar paslaugų prieinamumą (pvz. būtų absurdas jeigu robotas negalės atpažinti nusikaltėlio, kol „jis nedavė sutikimo“).

E3 ekspertas mano, jog reikalingas griežtesnis teisinis reglamentavimas ir pasekmių už šių duomenų praradimą / paviešinimą taikymas.

E4 ekspertas teigė jog šioje situacijoje praverstų technologinių sprendimų taikymo peržiūra ir vartotojų švietimo taikymas.

E5 ekspertas šiuo atveju konkrečios nuomonės ir pasiūlymų neturėjo.

Išvados: atsižvelgiant į ekspertų išsakytą nuomonę, kuri šiuo atveju šiek tiek išsiskiria, tačiau susitelkia ties biometrinių technologijų naudojimo nauda ir rizikomis asmens duomenų apsaugai bei privatumui. Svarbu, kad Lietuvoje būtų įvesti aiškūs, griežti teisės aktai, reglamentuojantys biometrinių technologijų naudojimą ir asmens duomenų apsaugą. Taip pat svarbu, kad visi subjektai, kurie tvarko asmens duomenis, laikytųsi šios tvarkos ir taikytų tinkamas saugumo priemones. Reikalingas didesnis vartotojų švietimo ir informavimo apie biometrinės technologijas skatinimas. Vartotojų informavimas apie galimas rizikas, siekiant padėti priimti informuotus ir savalaikius sprendimus galinčius apsaugoti asmens duomenų privatumą.

4.2. Etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims

Aktualiausios etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims rinkti ir tvarkyti. E1 eksperto nuomone aktualiausios etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims rinkti ir tvarkyti, yra susijusios su asmens privatumo ir diskriminacijos rizika. Ekspertas pažymi, jog šias problemas galima spręsti stiprinant reguliavimo ir priežiūros mechanizmus, rengiant tinkamas biometrinių technologijų naudojimo taisykles ir koncepcijas. Šiame etape turi būti atsižvelgiama į asmens teises ir gerąją praktiką, taip pat užtikrinamas atvirumas, bei skaidrumas biometrinių technologijų naudojimo procese.

E2 ekspertas mano, kad etinės problemos apima ne tik asmens identifikavimą, profiliavimą (kaip kokio gyvūno), bet ir šių duomenų padirbinėjimo ar priskyrimo kitiems asmenims, ar grupėms naudojant pvz. „deepfake“ technologijas atvejus. Visa tai gali padidinti labai kokybiškų „phishing“ atakų augimą ateityje, politinės nuomonės formavimą, asmenų sekimą ir kitus nusikaltimus. Eksperto pasiūlymas, kaip vienas iš būdų tvarkyti šias problemas, būtų - tikslus teisinis reguliavimas, naudotojų švietimas duomenų saugos tematika ir papildomų kontrolės priemonių taikymas.

E3 eksperto nuomone biometrinių duomenų atskleidimas reikštų asmens privatumo pažeidimą. Todėl siekiant spręsti galimas problemas, visų pirmą šios technologijos turėtų veikti taip, kad nebūtų rizikų atskleisti ar prarasti šios informacijos trečiosioms šalims.

E4 ekspertas pažymi jog, pagal biometrinius duomenys gali būti atskiriami tam tikros rasės asmenys, kas taip pat gali kelti atitinkamas problemas. Anot eksperto yra būtinas aiškus teisinis reglamentavimas šių duomenų valdymui ir naudojimui.

E5 ekspertas mano, kad viskas labai priklauso nuo to koks bus sukurtas teisinis reguliavimas, dėl šių duomenų rinkimo / saugojimo ir naudojimo.

Išvados: iš ekspertų pateiktų nuomonių galima išskirti keletą aktualiausių etinių problemų, susijusių su biometrinių technologijų naudojimui asmens duomenims rinkti ir tvarkyti. Tai yra asmens privatumo, diskriminacijos rizika, asmens identifikavimo, profiliavimo pavojus, biometrinių duomenų atskleidimo grėsmė, taip pat rizika, kad biometriniai duomenys gali būti naudojami tam tikros rasės asmenų atskyrimui. Ekspertai teigia, kad šias problemas galima spręsti stiprinant reguliavimo ir priežiūros mechanizmus, rengiant tinkamas biometrinių technologijų naudojimo taisykles ar koncepcijas, taip pat įgyvendinant tikslų teisinį reguliavimą. Pasitelkiant švietimą duomenų saugos tematika ir papildomas kontrolės priemones. Ekspertai siūlo užtikrinti atvirumą ir skaidrumą biometrinių technologijų naudojimo procese, siekiant atsižvelgti į tinkamą asmens teisių užtikrinimą ir gerąsias praktikas.

Dabartinės biometrinių technologijų situacijos Lietuvoje vertinimas, pagrindinės tendencijos ir iššūkiai. E1 ekspertas dabartinę biometrinių technologijų situaciją Lietuvoje vertina, kaip besiplečiančią, tačiau pabrėžia jog susiduriame su dideliais iššūkiais ir reikalavimais, susijusiais su asmens duomenų saugumu ir privatumu. Eksperto nuomone svarbiausios tendencijos yra biometrinių technologijų taikymas vis daugiau sričių, tobulinamos naujos technologijos ir spartus naudojimo sričių spektras. Galimus iššūkius ekspertas išskiria, susijusius su teisės aktų reikalavimais ir jų įgyvendinimu. Taip pat su didėjančiu susirūpinimu dėl asmens duomenų saugumo ir privatumo, kuri reikia užtikrinti, kad būtų išvengta duomenų nutekėjimų ir nelegalaus jų panaudojimo.

E2 ekspertas mano, jog biometrinės technologijos vis dar nėra labai plačiai paplitusios, bet joms žengiant į Lietuva bus vis daugiau klausimų ir problemų susijusių su šių duomenų apsauga ir naudojimu Lietuvoje.

E3 ekspertas teigia jog šiuo metu, labiausiai orientuojamasi į pirštų antspaudų, veido atpažinimo metodus. Ekspertas pažymi, jog vertinant tendencijas reikalinga analizuoti kas yra taikoma pasauliniu mastu.

E4 eksperto nuomone Lietuva yra maža, todėl didžiausią tendenciją darys bendra pasaulinė situacija.

E5 ekspertas teigia, jog nėra iki galo susipažinęs su informacija apie biometrinių technologijų panaudą Lietuvoje, todėl pakomentuoti situaciją susilaiko.

Išvados: iš šių ekspertų atsakymų galima daryti išvadas, kad biometrinių technologijų naudojimas Lietuvoje yra vis dar besiplečiantis, taip pat tikimasi, kad jis augs ir ateityje. Tačiau iš viso

to kyla tam tikri iššūkiai susiję su asmens duomenų saugumu ir privatumu, kaip teisės aktų reikalavimų rengimas, bei realus praktinis jų įgyvendinimo klausimas. Vertinant situaciją Lietuvoje, pastebima, kad biometrinės technologijos vis dar nėra plačiai paplitusios, tačiau joms žengiant į Lietuvą, neišvengiamai daugės problemų susijusių su šių duomenų apsauga ir tinkamu naudojimu atvejų kiekiai. Taip pat pastebima, kad Lietuva yra maža ir didžiausią tendenciją šių technologijų plėtrai, sudarys bendra pasaulinė situacija.

Teisinės ir reguliavimo sistemos šiuo metu Lietuvoje reglamentuojančios biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui. E1 eksperto teigimu, Lietuvoje biometrinių technologijų naudojimas asmens duomenų rinkimui ir tvarkymui reglamentuojamas bendrais teisinais aktais, tokiais kaip Europos Sąjungos duomenų apsaugos reglamentas (GDPR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, bei atitinkamais sektoriaus teisės aktais. Taip pat ekspertas pabrėžia, jog yra parengtos koncepcijos ir gairės, reglamentuojančios biometrinių technologijų taikymą, pvz., Valstybinės duomenų apsaugos inspekcijos rekomendacijos ir Krypties gairės. Eksperto manymu, šios teisinės ir reguliavimo sistemos yra pagrindas asmens duomenų saugumui ir privatumui užtikrinti, tačiau jų veiksmingumas priklauso nuo jų įgyvendinimo ir priežiūros mechanizmų efektyvumo. Ekspertas taip pat pažymi, jog pastaraisiais metais padaryta didžiulė pažanga, kadangi Lietuva įgyvendino „BDAR“ ir atitinkamus sektorinius teisės aktus, kurie užtikrina gerąją praktiką ir standartus asmens duomenų rinkimo ir tvarkymo srityje. Eksperto nuomone, šiuo metu Lietuvoje teisinės ir reguliavimo sistemos atitinka pagrindinius reikalavimus asmens privatumo teisių apsaugai, tačiau vis dar yra kam skirti dėmesio, siekiant užtikrinti jų veiksmingumą.

E2 teigia, kad šiuo metu Lietuvoje veikia Europos sąjungoje išleistas Bendrasis duomenų apsaugos reglamentas (BDAR), kuriame dalinai yra apibrėžiamas biometrinių duomenų (specialiu techniniu apdorojimu gauti asmens duomenys) naudojimas. Kaip pažymi ekspertas reglamentas apibrėžia biometrinius duomenis, tačiau jų labai plačiai nedetalizuoja.

E3 ekspertas teigia, jog nėra visiškai įsigilinęs į Lietuvoje esančius teisės aktus, todėl plačiau pakomentuoti susilaiko. Tačiau eksperto nuomone, asmens privatumo teisių neapsaugo net „ADA“ teisės aktai, todėl ekspertas mano, kad situacija su biometriniais duomenimis yra daug prastesnė.

E4 ekspertas išskiria bendrąjį duomenų apsaugos reglamentą. Taip pat pažymi, jog nėra išsamiai susipažinęs su „BDAR“ ir lydinčių teisės aktų efektyvumu ir spragomis, todėl plačiau pakomentuoti taip pat susilaiko.

E5 ekspertas teigė, jog taip pat nėra visiškai įsigilinęs į Lietuvoje esančius teisės aktus ir teisinį reguliavimą.

Išvados: remiantis dalies ekspertų nuomone ir pateiktomis įžvalgomis, siekiant Lietuvoje tinkamai spręsti biometrinių technologijų keliamus iššūkius, svarbu atnaujinti arba sugriežtinti esamus

duomenų apsaugos ir privatumo įstatymus. Vien tik „BDAR“ taikymas dalies ekspertų nuomone, nėra pakankamas, o esamos teisinės reguliavimo sistemos Lietuvoje atitinka tik pagrindinius reikalavimus. Papildomų ar esamų sprendimų peržiūra, turėtų apimti aiškiai apibrėžtus jautrius asmens duomenis, nustatyti griežtus reikalavimus duomenų rinkimui, tvarkymui ir saugojimui, sukurti aiškias taisykles, dėl biometrinių technologijų naudojimo tikslų, apribojimų, ar galimų pasekmių. Dalies ekspertų tarpe taip pat išryškėjo įsigilinimo į teisinį reguliavimą poreikio ir žinių stoka.

Galimybės atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus, siekiant spręsti unikalios biometrinių technologijų keliamus iššūkius. E1 eksperto nuomone, duomenų apsaugos ir privatumo įstatymai turėtų būti atnaujinami ir prisitaikoma prie naujų iššūkių, susijusių su biometrinėmis technologijomis. Tam, kad būtų galima spręsti unikalios biometrinių technologijų keliamus iššūkius, būtina:

- aiškiai apibrėžti, kokie asmens duomenys yra laikomi jautria informacija, kuri turi būti apsaugota;
- nustatyti griežtus reikalavimus, dėl asmens duomenų rinkimo, tvarkymo ir saugojimo, taip užtikrinant asmens privatumą ir saugumą;
- užtikrinti, kad vartotojams būtų suteikta pakankamai informacijos apie jų duomenų tvarkymą, įskaitant informaciją apie biometrines technologijas ir jų naudojimą;
- sukurti aiškias taisykles, dėl biometrinių technologijų naudojimo tikslų, apribojimų ir pasekmių;
- nustatyti griežtas baudas už pažeidimus, susijusius su asmens duomenų apsauga ir privatumu;
- užtikrinti, kad būtų laikomasi taisyklių, susijusių su duomenų perdavimu trečiosioms šalims, ypač užsienio valstybėms;
- užtikrinti, kad vartotojai turėtų teisę reikalauti, kad jų duomenys būtų panaikinti arba perduoti kitiems subjektams;
- stebėti naujoves ir tendencijas susijusias su biometrinėmis technologijomis, laiku atnaujinti taisykles, kad būtų galima atsižvelgti į naujus iššūkius ir galimas rizikas.

Kaip veiksmingiausius vykdymo užtikrinimo mechanizmus ekspertas pažymi, griežtų audito ir stebėjimo procesų, atliekamų atitinkamų institucijų, kurios užtikrintų, kad biometrinių technologijų naudojimas atitinka teisės aktus ir yra saugūs vartotojams proceso vykdymą. Taip pat pažymi, jog yra svarbu turėti tinkamas sankcijas ir baudas, kad būtų galima pažaboti bet kokius galimus pažeidimus.

E2 ekspertas mano, jog Lietuvoje atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus, būtų galima tik Europos sąjungos kontekste. Ekspertas teigia, kad realiausias variantas būtų plačiau detalizuoti ir tikslinti biometrinių technologijų apibrėžimą ir panaudojimą teisiniuose dokumentuose (kad ir plėsti tą patį BDAR ar išleisti naują papildantį dokumentą konkrečiai, dėl Biometrinių technologijų). Tačiau kaip pažymi ekspertas, toks teisinis reguliavimas tikriausiai

tinkamai veiktų tik nuolat koreguojamas ir vykdomas neatsiliekant nuo technologijų vystymosi spartos.

E3 eksperto nuomone, biometrinių duomenų apsaugos nereikėtų tapatinti su asmens duomenimis. Taip pat ekspertas pažymi, jog biometrinių technologijų panaudojimas ir duomenų atskleidimas gali turėti didesnės žalos, būtent, dėl šios priežasties eksperto manymu, apsaugos taikymas turėtų būti griežtesnis.

E4 ir E5 ekspertai teigia neturintys aiškių pasiūlymų, dėl galimybių atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus.

Išvados: ekspertų nuomone yra būtina atnaujinti duomenų apsaugos ir privatumo įstatymus, prisitaikant prie naujų biometrinių technologijų keliamų iššūkių. Tam reikalinga aiškiai apibrėžti galimai jautrią informaciją, nustatyti griežtus reikalavimus asmens duomenų rinkimui, tvarkymui ir saugojimui. Vartotojams turi būti suteikta pakankamai informacijos apie jų duomenų tvarkymą ir biometrinių technologijų naudojimą. Svarbu sukurti aiškias taisykles, dėl biometrinių technologijų naudojimo, nustatyti griežtas baudas už pažeidimus. Ekspertai pabrėžia, kad tinkamas teisinis reguliavimas yra labai svarbus, tačiau jis turi būti nuolat koreguojamas ir vykdomas neatsiliekant nuo technologijų vystymosi. Galiausiai yra svarbu atskirti biometrinius duomenis nuo bendros asmens duomenų politikos, taikant griežtesnes apsaugos priemones.

4.3. Vartotojų švietimo ir informuotumo didinimo kampanijos

Vaidmuo tenkantis vartotojų švietimui ir informuotumo didinimo kampanijoms, siekiant informuoti Lietuvos visuomenę apie biometrinių technologijų tinkamą naudojimą, bei sąlygojamas grėsmes. E1 eksperto manymu, vartotojų švietimas ir informuotumo didinimo kampanijos yra labai svarbios, siekiant informuoti visuomenę apie biometrinių technologijų teisingą ir atsakingą naudojimą, bei jų sąlygojamas grėsmes. Vartotojams reikia suprasti, kaip biometrinės technologijos veikia, kaip jų duomenys yra naudojami, ir kokie yra jų teisės susijusios su asmens duomenų saugumu ir privatumu. Veiksmingiausia strategija eksperto nuomone, būtų nuolat informuoti vartotojus apie biometrinių technologijų naudojimą, jų pranašumus ir trūkumus, taip pat reikėtų informuoti apie galimas grėsmes ir sprendimus, kuriuos jie gali priimti, norėdami apsaugoti savo duomenis. Švietimo kampanijas reikėtų organizuoti viešai, internete ir socialinėje medijoje, taip pat reikėtų remtis valdžios institucijų ir nevyriausybinų organizacijų informacijos sklaidos iniciatyvomis.

E2 eksperto nuomone, vartotojų švietimas asmens duomenų saugos tematika yra būtinas, tačiau net ir esant vartotojų švietimui, visko apsaugoti nepavyks - biometriniai duomenys gali būti renkami ir slapta tiek fizinėmis priemonėmis, tiek ir IT technologijų dėka, kai jie yra skaitmenizuoti. Ekspertas taip pat pabrėžia, kad įstatymai nesaugo nuo tokių duomenų rinkimo privačiais reikalais.

E3 ekspertas, teigia, kad švietimas yra būtinas. Anot eksperto, be jo visuomenės palankumo šioms technologijoms ir jų priėmimo nepasieksime. Žmonės turi suprasti kas tai yra ir jiems reikia padėti tai padaryti.

E4 eksperto nuomone, švietimas užima kritinį vaidmenį, tai yra labai jautri ir kontraversiška tema, dėl to reikės delikačios ir ilgalaikės komunikacijos strategijos, bei labai gerai apgalvotų teisės aktų.

E5 ekspertas mano, jog švietimas turi būti pateikiamas suprantamai, o vartotojai aiškiai informuojami, kur ir kaip jų duomenys bus panaudoti.

Išvados: vartotojų švietimas ir informavimo kampanijos yra būtinos, siekiant informuoti visuomenę apie biometrinių technologijų tinkamą naudojimą ir susijusias grėsmes. Vartotojams reikia suprasti, kaip biometrinės technologijos veikia, kaip jų duomenys yra naudojami ir kokios yra jų teisės susijusios su asmens duomenų saugumu ir privatumu. Veiksmingiausia strategija būtų nuolat informuoti vartotojus apie biometrinių technologijų naudojimą, jų pranašumus ir turimus trūkumus, galimas grėsmes, kas suteiktų galimybes priimti tinkamus sprendimus, siekiant apsaugoti savo asmens duomenis. Švietimo kampanijas reikėtų organizuoti viešai, internete, socialinėje medijoje, taip pat reikėtų remtis valdžios institucijų ir nevyriausybinių organizacijų informacijos sklaidos iniciatyvomis. Švietimas yra būtinas, siekiant priimti tinkamus ir atsakingus sprendimus, tuo pačiu, kad visuomenė galėtų geriau suprasti biometrinių technologijų pranašumus ir trūkumus. Vartotojams švietimas turėtų būti pateikiamas suprantamai, o aiškiai reglamentuojant ir informuojant, apie asmens duomenų panaudojimą.

4.4. Pramonės savireguliacija ir jos vaidmuo

Pramonės savireguliacijos vaidmuo, skatinant atsakingą biometrinių technologijų naudojimą. E1 eksperto nuomone, pramonės savireguliacija gali atlikti svarbų vaidmenį skatinant atsakingą biometrinių technologijų naudojimą, nes tai padeda organizacijoms savarankiškai spręsti etines ir teises problemas. Veiksmingos savireguliacijos sistemos sudedamosios dalys kaip pažymi ekspertas, yra aiškos ir suprantamos taisyklės ir reikalavimai, nuolatinis stebėjimas ir kontrolė, skaidrumas ir atvirumas, taip pat atsakomybė už pažeidimų prevenciją ir nuolatinį tobulinimą.

E2 ekspertas mano, jog galima pamiršti pramonės savireguliaciją, jei nėra įpareigojančių teisės aktų. Savireguliacija reikalaus verslo išlaidų, o verslas tai tiesiog ignoruos. Ekspertas pažymi, kad tai būtų būdinga, bent jau didžiajai verslo daliai, nes verslo tikslas yra gauti kuo didesnę pelną, maksimaliai supaprastinant gamybos procesą.

E3 eksperto nuomone, pramonės savireguliacijoje, bet kuriuo atveju daugiau bus orientuojamasi tik į pelną (su galimomis retomis išimtimis), visus saugumo reikalavimus bandanti atitikti bent minimaliajai daliai, ar tik tiek kiek tai teisiškai yra reguliuojama.

E4 ekspertas teigia, jog savireguliacija turi veikti pagal aiškiai standartizuotus ir visiems vienodai taikomus principus. Taip pat ekspertas pažymi, jog turi būti taikomos papildomos kontrolės priemonės.

E5 ekspertas teigia, pirma kartą girdintis, jog privatus verslo subjektas turi savireguliacijos mechanizmus, todėl pakomentuoti pramonės savireguliacijos vaidmens negalintis.

Išvados: kiekvienas ekspertas turi savo požiūrį į pramonės savireguliacijos vaidmenį. Keli ekspertai mano, kad savireguliacija gali padėti organizacijoms spręsti etines ir teisinių problemas, tačiau kiti svarsto, kad viso to nepakanka ir žvelgiant iš praktinės pusės reikalingi įpareigojantys teisės aktai. Galima daryti prielaidą, jog pramonės savireguliacija neturėtų būti vienintelis sprendimas, ar vienintelis kelias į atsakingą biometrinių technologijų naudojimą, tai turėtų būti tik viena iš daugelio galimų priemonių skirtų spręsti biometrinių technologijų problemas.

4.5. Biometrinių technologijų ateitis

Biometrinių technologijų naudojimo Lietuvoje vystymasis artimiausiais metais ir poveikis asmens duomenų saugumo ir privatumo užtikrinimui. E1 eksperto nuomone, atsižvelgiant į tai, kad biometrinės technologijos yra sparčiai tobulėjančios ir plintančios, jų naudojimas Lietuvoje artimiausiais metais tikriausiai augs. Kaip pažymi ekspertas, tai gali turėti neigiamą poveikį asmens duomenų saugumui ir privatumui, jei nebus atsižvelgiama į anksčiau išsakytas problemas ir netaikant tinkamo jų adresavimo. Ekspertas taip pat pakartoja, jog, tam, kad būtų užtikrintas asmens duomenų saugumas, būtina įdiegti patikimas ir veiksmingas duomenų apsaugos mechanizmus, taip pat svarbu didinti vartotojų informuotumą ir sąmoningumą.

E2 ekspertas mano, kad artimiausiais metais biometrinių technologijų naudojimas Lietuvoje vystysis panašiu tempu kaip vakarų šalyse. Sparčiausiai vystysis kartu su IT technologijų sritimi – tikėtina, kad didės biometrinių duomenų rinkimo mastai, daugės privatumo grėsmių atsirandančių iš biometrinių duomenų nutekėjimo, didės tokių technologijų kaip „deepfake“ poveikio piratavimui (pvz., išpirkos reikalavimas už sumontuoto siužeto neviešinamą ir pan.) ir propagandos bei suklastotų nuomonių skelbimų atvejai. Kaip pažymi ekspertas, dėl vėluojančio biometrinių duomenų reglamentavimo tiek įmonės, tiek žmonės įsitrauks į šių technologijų platų naudojimą (pvz. atsiskaitymas už prekes, be piniginių ar telefono), kas dar labiau apsunkins jų griežtesnio reglamentavimo taikymą.

E3 eksperto nuomone biometrinių technologijų naudojimo Lietuvoje vystymasis artimiausiais metais bus proporcingas kitoms taikomoms technologijoms ir plėsis lygiagrečiai su visomis.

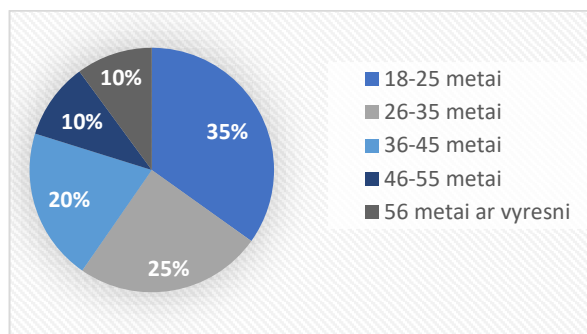
E4 ekspertas, dėl biometrinių technologijų naudojimo Lietuvoje vystymosi, nuomonės neturėjo.

E5 eksperto teigimu biometrinių technologijų naudojimo Lietuvoje vystymasis artimiausiais metais vyks pakankamai lėtai ir vangiai.

Išvados: ekspertų nuomonės, dėl Lietuvoje naudojamų biometrinių technologijų vystymosi artimiausiais metais ir poveikio asmens duomenų saugumui, bei privatumui yra įvairios. Keli ekspertai mano, kad biometrinių technologijų naudojimas Lietuvoje ir toliau augs, tačiau kiti mano, kad vystymasis bus lėtas, arba proporcingas kitoms IT technologijoms.

4.6. Lietuvos vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą tyrimo rezultatai

Atliekant vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą tyrimą, pačioje pradžioje buvo siekiama nustatyti respondentų dalyvavusių apklausoje amžiaus grupes. Iš viso tyrime sudalyvavo 218 respondentų, kurie pasiskirstė po skirtingas amžiaus grupes. Esantys amžiaus skirtumai, skirtingose amžiaus grupėse gali perteikti skirtingą požiūrį į turimas žinias, įpročius, ar patirtis susijusias su naujų technologijų taikymu ir naudojimu. Jaunesnės kartos atstovai gali būti labiau linkę pasitikėti naujomis technologijomis ir jas lengviau priimti. Vyresnės kartos žmonės, priešingai, šiuo atveju gali būti atsargesni, ar turėti didesnį susirūpinimą, dėl asmens duomenų saugumo ir šių technologijų naudojimo (žr. 5 pav.).

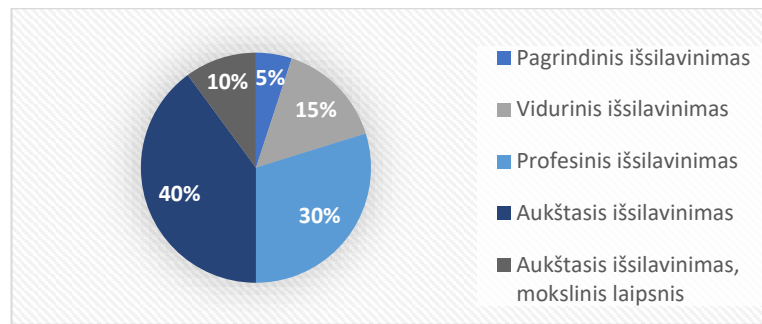


Šaltinis: parengtas autoriaus

5 pav. Amžiaus pasiskirstymas

Iš pateiktos diagramos, matome, kad didžioji dalis apklausoje dalyvavusių respondentų priklauso 18-25 metų amžiaus grupei, viso 35 proc. (76 respondentai). Šiai grupei priklausančių apklausos dalyvių skaičius buvo didžiausias. Kiek mažiau 25 proc. (54 respondentai) atsakiusiųjų, sudarė 26-35 metų grupę. Toliau sekė, 20 proc. (44 respondantai), sudarantys 36-45 metų grupę. Likusią dalį dalinosi 46-55 (22 respondantai) ir 56 ar vyresnio amžiaus (22 respondantai) respondentų grupės, kurios pasiskirstė po 10 proc., bendrai sudarydamos likusius 20 proc. apklaustųjų.

Siekiant nustatyti respondentų išsilavinimo laipsnį, apklausoje buvo pateikiamas klausimas „Koks yra Jūsų išsilavinimas?“ (žr. 6 pav.).

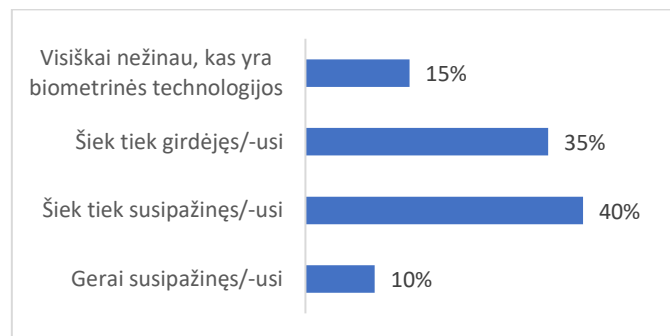


Šaltinis: parengtas autoriaus

6 pav. Išsilavinimo laipsnio pasiskirstymas

Diagramoje matome, jog daugiausiai respondentų turi aukštąjį išsilavinimą, kas sudaro 40 proc. (87 respondentai) atsakiusių grupę. Profesinį išsilavinimą turinčių respondentų grupę sudarė 30 proc. (65 respondentai). Respondentų turinčių aukštąjį ir profesinį išsilavinimą kiekis sudarė per 70% visų gautų atsakymų. Vidurinį išsilavinimą turinčių respondentų grupę sudarė 15 proc. (33 respondentai), o pagrindinį išsilavinimą turėjo tik 5 proc. (11 respondentai) atsakiusių. Taip pat pastebima, jog 10 proc. (22 respondentai) turėjo aukštąjį išsilavinimą ir mokslinį laipsnį, tai reiškė, kad yra baigę magistrantūros ar doktorantūros studijas.

Siekiant nustatyti, kiek gerai respondentai yra susipažinę su biometrinėmis technologijomis, apklausoje buvo pateiktas klausimas „Kiek gerai esate susipažinę su biometrinėmis technologijomis?“ (žr. 7 pav.).

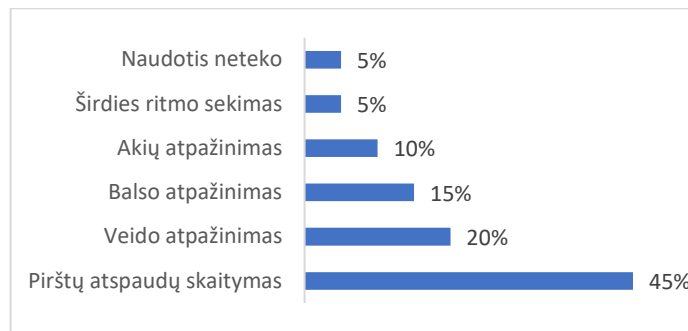


Šaltinis: parengtas autoriaus

7 pav. Susipažinimas su biometrinėmis technologijomis

Iš gautų atsakymų matome, kad tik 10 proc. (22 respondentai) atsakiusių yra gerai susipažinę su biometrinėmis technologijomis, o dauguma, net 40 proc. (87 respondentai), yra tik šiek tiek susipažinę. 35 proc. (78 respondentai) pažymėjo, jog apie šias technologijas yra tik šiek tiek girdėję, o net 15 proc. (33 respondentai) net nežino, kas tai yra.

Siekiant nustatyti biometrinių technologijų naudojimo pasiskirstymą, apklausoje buvo užduotas klausimas „Kurias biometrines technologijas jau esate naudoję/-usi savo kasdieninėje veikloje?“ (žr. 8 pav.).

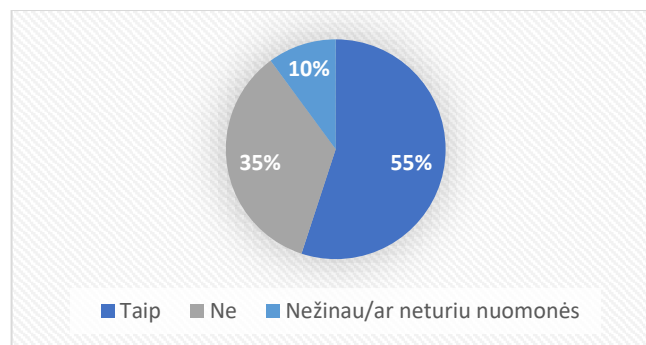


Šaltinis: parengtas autoriaus

8 pav. Biometrinių technologijų naudojimo pasiskirstymas

Rezultatai parodė, kad dauguma respondentų 45 proc. (98 respondentai) yra naudoję arba naudojami pirštų atspaudų skaitymo technologija. Toliau pagal naudojimo dažnumą sekė veido atpažinimo technologija, kurią nurodė naudoję, ar naudoja 20 proc. (44 respondentai) apklaustųjų. Kiek mažiau naudojusią ar naudojančią, buvo balso atpažinimo technologiją, 15 proc. (33 respondentai) apklaustųjų. Tarp mažiausiai paplitusių biometrinių technologijų, respondentų tarpe buvo akių atpažinimo 10 proc. (22 respondentai) ir širdies ritmo sekimo 5 proc. (11 respondentų), o likę 5 proc. (11 respondentų) nurodė, jog nebuvo naudoję jokių biometrinių technologijų.

Siekiant nustatyti, ar respondentai naudojami biometrinėmis technologijomis savo įrenginiuose, apklausoje buvo pateiktas klausimas „Ar naudojate biometrines technologijas savo įrenginiuose (pvz., išmaniajame telefone ar kompiuteryje)?“ (žr. 9 pav.).

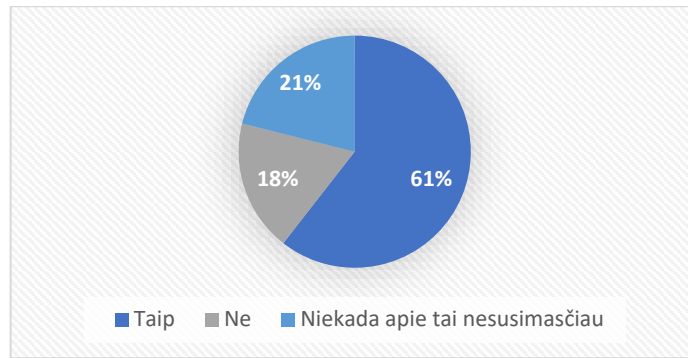


Šaltinis: parengtas autoriaus

9 pav. Biometrinės technologijų įrenginiuose naudojimas

Rezultatai parodė, kad dauguma respondentų, net 55 proc. (120 respondentai), kas yra šiek tiek daugiau nei pusė apklaustųjų, naudojami biometrinėmis technologijomis savo įrenginiuose. Likusi dalis per 35 proc. (76 respondentai) nurodė šių technologijų asmeniniuose įrenginiuose nenaudojantys, o 10 proc. (22 respondentai) pažymėjo nežinantys ar neturintys nuomonės šiuo klausimu.

Siekiant nustatyti respondentų nuomonę saugumo klausimu, dėl biometrinių technologijų ir tradicinių tapatybės nustatymo priemonių naudojimo, apklausoje buvo pateiktas klausimas „Ar manote, kad biometrinės technologijos yra saugesnės nei tradicinės tapatybės patvirtinimo priemonės (pvz., slaptažodžiai)?“ (žr. 10 pav.).

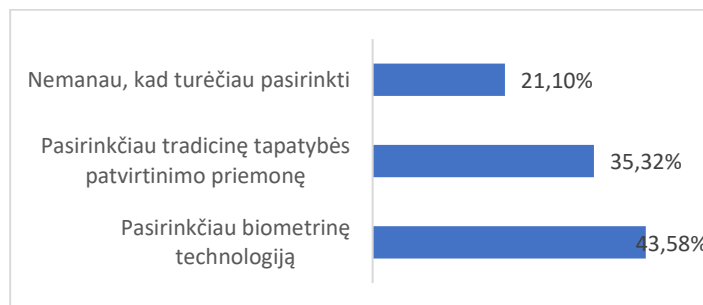


Šaltinis: parengtas autoriaus

10 pav. Biometrinių technologijų saugumo palyginimas su tradicinėmis tapatybės nustatymo priemonėmis

Diagramoje matome, jog daugiau nei puse apklaustųjų 61 proc. (132 respondentai) nurodė manantys, kad biometrinės technologijos yra saugesnės, lyginant su tradicinėmis asmens tapatybės autentifikavimo priemonėmis. Tik maža dalis, 18 proc. (40 respondentų) nurodė manantys priešingai, o 21 proc. (46 respondentai), pažymėjo faktą, kad apie tai niekada nėra susimąstę.

Siekiant nustatyti respondentų nuomonę, tapatybės patvirtinimo priemonių pasirinkimo pirmenybės teikime, biometrinių technologijų, ar tradicinių autentifikavimo metodų naudojime, apklausoje buvo pateiktas klausimas „Jei galėtumėte pasirinkti tarp tradicinės tapatybės patvirtinimo priemonės (pvz., slaptažodžio) ir biometrinės technologijos, kurią pasirinktumėte?“ (žr. 11 pav.).

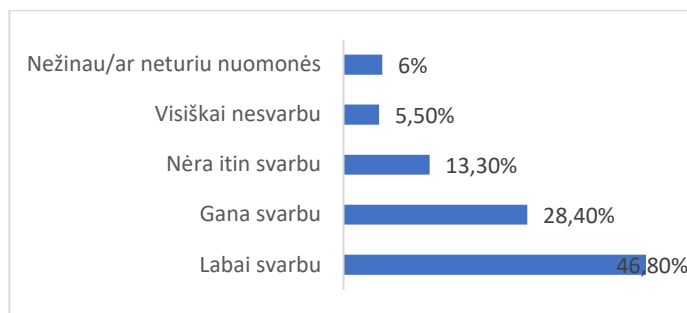


Šaltinis: parengtas autoriaus

11 pav. Tapatybės patvirtinimo priemonių pirmenybės teikimo pasiskirstymas

Iš gautų atsakymų matome, kad didesnė dalis respondentų 43,58 proc. (95 respondentai) linkę rinktis biometrinę technologiją tapatybės patvirtinimui, jeigu tokia galimybė būtų. Kiek mažiau 35,32 proc. (77 respondentai) mano jog pasirinktą tradicinio tipo tapatybės patvirtinimo priemonę. Likusi dalis 21,10 proc. (46 respondentai) mano, jog neturėtų turėti pasirinkimo galimybių, sprendžiant kurią technologiją naudoti.

Siekiant nustatyti respondentų nuomonę, biometrinių duomenų naudojimo ir rinkimo kontrolės svarba, apklausoje buvo pateiktas klausimas „Kiek svarbu, kad Jūs turėtumėte kontrolę, dėl savo biometrinių duomenų rinkimo, saugojimo ir naudojimo?“ (žr. 12 pav.).

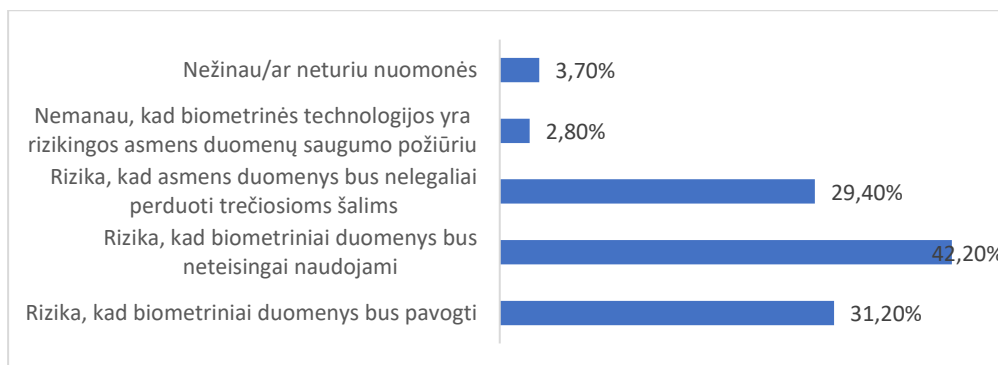


Šaltinis: parengtas autoriaus

12 pav. Biometrinių duomenų rinkimo, saugojimo ir naudojimo kontrolės svarba

Rezultatai parodė, kad daugumai respondentų rūpi kontrolės mechanizmų taikymo svarba, 46,80 proc. (102 respondentai), nurodė, kaip labai svarbų aspektą. Mažesnę dalis kurią sudarė 28,40 proc. (62 respondentai) išskyrė kaip gana svarbų. Likusi dalis 13,30 proc. (29 respondentai) pažymėjo, jog kontrolės svarba biometrinių duomenų rinkimo, saugojimo ir naudojimo prasme yra ne itin svarbi, o 5,50 proc. (12 respondentai) pažymėjo kaip visiškai nesvarbią. Nežinančių ar neturinčių nuomonės šiuo klausimu buvo tik 6 proc. (13 respondentų).

Siekiant nustatyti respondentų nuomonę, apie galimas pagrindines biometrinių technologijų naudojimo rizikas, apklausoje buvo pateiktas klausimas „Kokias pagrindines rizikas matote naudojantis biometrinėmis technologijomis asmens duomenų saugumo požiūriu?“, su galimybe pasirinkti daugiau nei vieną galimą atsakymą (žr. 13 pav.).

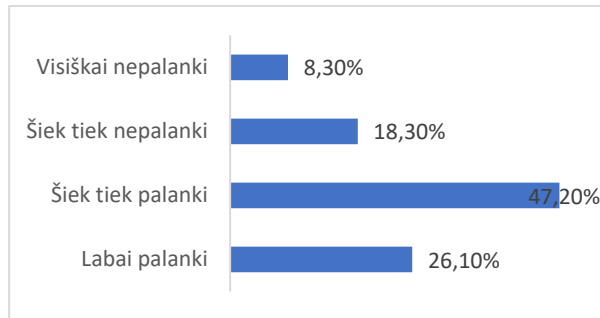


Šaltinis: parengtas autoriaus

13 pav. Pagrindinės rizikos biometrinių technologijų naudojimo kontekste

Iš pateiktų atsakymų matome, kad didžioji dalis respondentų su galimomis rizikomis naudojantis biometrinėmis technologijomis proporcingai yra linkę sutikti. Respondentų nuomonė renkantis daugiau nei vieną galimą riziką išliko gana panaši, su nedideliu skirtumu. Su rizika, kad asmens duomenys gali būti nelegaliai perduoti trečiosioms šalims, pasirinkimai siekė 29,40 proc. Su rizika, kad biometriniai duomenys gali būti pavogti, pasirinkimai siekė šiek tiek didesnę kiekį, 31,20 proc. Daugiausia respondentų tarpe pasirinkta rizika buvo, neteisingas biometrinių duomenų naudojimas, 42,20 proc. Likusi dalis pasirinkimų, 2,80 proc. numatė jog biometrinės technologijos nėra rizikingos, o 3,70 proc. sudarė nuomonės neturinčių, ar nežinančių respondentų pasirinkimai.

Siekiant nustatyti bendrą respondentų požiūrį į biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui, apklausoje buvo pateiktas klausimas „Kokia yra jūsų bendra nuomonė apie biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui?“ (žr. 14 pav.).



Šaltinis: parengtas autoriaus

14 pav. Nuomonė biometrinių technologijų naudojimo asmens duomenų rinkimui ir tvarkymui kontekste

Rezultatai parodė, jog didžiosios dalies respondentų požiūris į biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui yra šiek tiek palankus, arba kitaip tariant palankus, net 47,20 proc. (103 respondentai). Kaip labai palankų sprendimą pasirinko santykinai maža dalis, tik 26,10 proc. (57 respondentai). Turintys mažą palankumą nurodė 18,30 proc. (40 respondentų), o visiškai nepalankią nuomonę sudarė, 8,30 proc. (18 respondentų) pasirinkimai.

Siekiant nustatyti bendrą respondentų požiūrį, bei nuomonės proporcijas į galimus iššūkius ir rizikos veiksnius siejamus su biometrinėmis technologijomis Lietuvoje, apklausoje buvo pateiktas klausimas „Kokius matote galimus pagrindinius iššūkius ir rizikos veiksnius susijusius su biometrinėmis technologijomis Lietuvoje?“ (žr. 15 pav.).



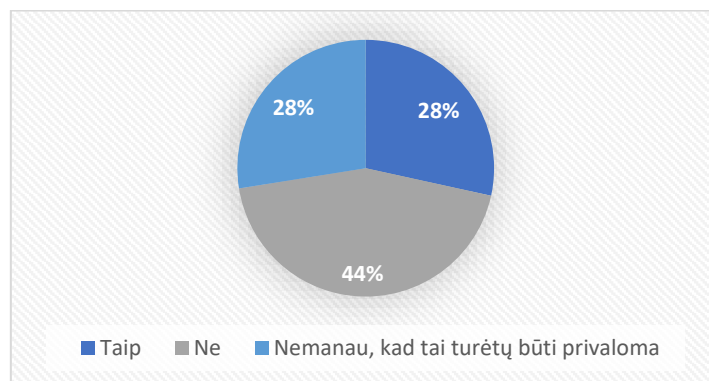
Šaltinis: parengtas autoriaus

15 pav. Iššūkiais ir rizikos veiksniais siejami su biometrinėmis technologijomis Lietuvoje

Šiuo atveju respondentai galėjo pasirinkti daugiau nei vieną galimą variantą. Iš gautų rezultatų matome, kad daugiausiai pasirinkimų turėjo duomenų vagystės ir sukčiavimo atvejai, 51,38 proc. ir

reguliavimo trūkumas, net 43,12 proc. Atitinkamai respondentai rinkosi ir biometrinių duomenų galimybę būti suklastotiems ar pakoreguotiems riziką, 37,16 proc., taip pat kiek mažiau rinkosi netinkamo biometrinių duomenų saugojimo atvejų riziką, 32,57 proc. Mažesnę dalį pasirinkimų sudarė, asmeninių duomenų rinkimo kiekio skaitmeninėje erdvėje didėjimo tendencijos rizika, 19,27 proc. Likusi dalis, 9,17 proc. (20 respondentų) nurodė kitus veiksnius. Dalis kitas priežastis pasirinkusių respondentų, kaip galimas rizikas ir iššūkius akcentavo, nepakankamą informacijos srautą, bei švietimą apie biometrines technologijas Lietuvoje. Taip pat dalis respondentų manė, kad bus susiduriama su kontrolės mechanizmų taikymo problemomis, reguliavimo trūkumais, netinkamo, ar neteisėto biometrinių technologijų panaudojimo atvejais ir mažu skaidrumu įmonių tarpe. Kai kurie respondentai iškėlė susirūpinimą biometrinių technologijų naudojimo poveikiu socialinėje terpėje su galimomis neigiamomis pasekmėmis.

Siekiant nustatyti respondentų nuomonės santykį, dėl privalomos būtinybės vertinti viešojo ir privataus sektoriaus įmones, apklausoje buvo pateiktas klausimas „Ar manote, kad viešosios institucijos ir privačios įmonės turėtų būti privalomai vertinamos pagal jų asmens duomenų saugumo politiką ir naudojamas biometrines technologijas?“ (žr. 16 pav.).

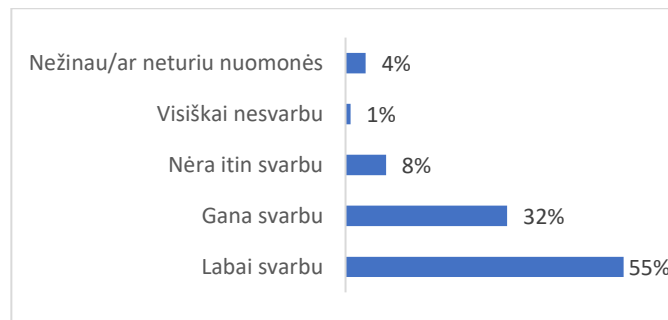


Šaltinis: parengtas autoriaus

16 pav. Nuomonė, dėl viešojo ir privataus sektoriaus įmonių privalomo vertinimo

Rezultatai parodė, jog didžiosios dalies respondentų nuomone privalomas viešojo ir privataus sektoriaus įmonių vertinimas nėra būtinas, už tai pasisakė 44 proc. (96 respondentai). Likusi dalis atsakymų pasiskirstė po lygiai, skirtumas pasireiškė kelių respondentų nuomonėje. Jog toks vertinimas turėtų būti taikomas, nuomonę pareiškė 28 proc. (62 respondentai). Manantys, kad tokio privalomo vertinimo neturėtų būti, atsakymų sudarė 28 proc. (60 respondentų).

Siekiant nustatyti respondentų nuomonę, dėl įmonių asmens duomenų tvarkymo praktikos viešinio politikos, apklausoje buvo pateiktas klausimas „Kiek Jums svarbu, kad įmonės, kurios naudoja biometrines technologijas, informuotų apie savo asmens duomenų tvarkymo praktikas?“ (žr. 17 pav.).

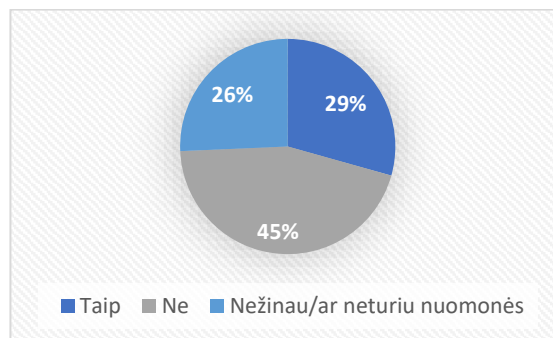


Šaltinis: parengtas autoriaus

17 pav. Nuomonė, dėl įmonių asmens duomenų tvarkymo praktikos viešinimo

Rezultatai parodė, jog didžiosios dalies respondentų nuomone įmonių asmens duomenų tvarkymo praktikos viešinimas yra labai svarbus aspektas, už tai pasisakė 55 proc. (120 respondentų), kad tai yra gana svarbu nuomonė išreiškė, 32 proc. (70 respondentų). Likusi dalis apklaustųjų, 8 proc. (17 respondentų) pasisakė, jog įmonių asmens duomenų tvarkymo praktikos viešinimas nėra itin svarbus aspektas, o 1 proc. (2 respondentai) pažymėjo, kaip visiškai nesvarbią praktiką. Likusi dalis respondentų, 4 proc. (9 respondentai) pažymėjo, kaip nežinantys ar neturintys nuomonės, dėl tokios praktikos taikymo poreikio.

Tolimesniame apklausos etape buvo siekiama nustatyti respondentų pasitikėjimo įmonių naudojančių biometrines technologijas, tinkamu asmens duomenų saugojimu. Apklausoje pateikiant klausimą „Ar Jūs pasitikite įmonių naudojančių biometrines technologijas tinkamu asmens duomenų saugojimu?“ (žr. 18 pav.).



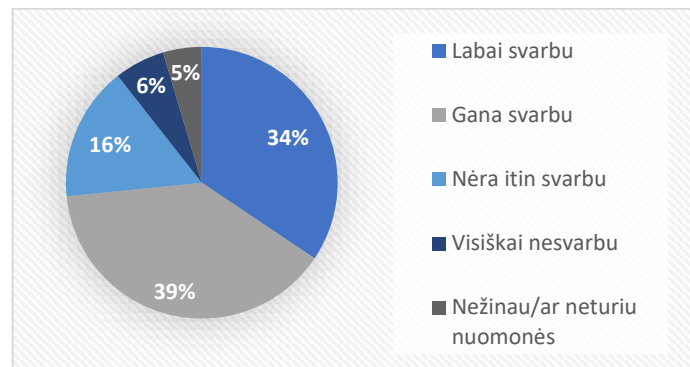
Šaltinis: parengtas autoriaus

18 pav. Pasitikėjimas įmonių tinkamu asmens duomenų saugojimu

Rezultatai parodė, jog didžioji dalis respondentų, nepasitiki įmonių naudojančių biometrines technologijas tinkamu asmens duomenų saugojimu, kas sudarė 45 proc. (98 respondentai) apklaustųjų. Pasitikinčių įmonėmis dalis, siekė tik 29 proc. (64 respondentai), o likusi dalis, 26 proc. (56 respondentai) pažymėjo, kaip nežinantys ar neturintys nuomonės šiuo klausimu.

Siekiant nustatyti respondentų nuomonę, dėl galimybių kontroliuoti savo biometrinių duomenų naudojimą, apklausoje buvo pateiktas klausimas „Kiek Jums yra svarbu, kad būtų suteikta galimybė

kontroliuoti savo biometrinių duomenų naudojimą (pvz., galimybė atšaukti savo suteiktą sutikimą)?“ (žr. 19 pav.).

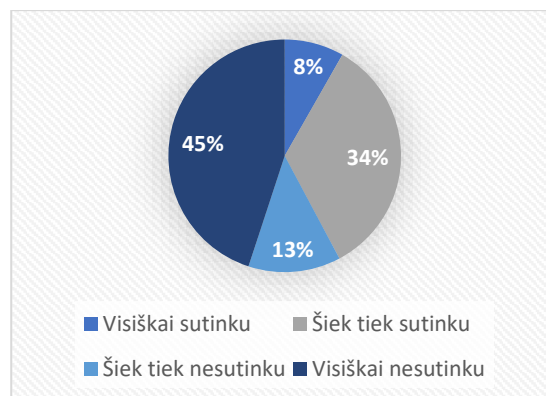


Šaltinis: parengtas autoriaus

19 pav. Galimybė kontroliuoti savo biometrinių duomenų naudojimą

Iš rezultatų matome, jog galimybė kontroliuoti savo biometrinių duomenų naudojimą, labai svarbi yra 34 proc. (75 respondentai) apklaustųjų ir kaip gana svarbią, pažymį, 39 proc. (85 respondentai) apklaustųjų. Kaip ne itin svarbų aspektą nurodė, 16 proc. (35 respondentai), visiškai nesvarbi galimybė buvo, 6 proc. (13 respondentų) apklaustųjų, likusi dalis 5 proc. (10 respondentų) nurodė nežinantys ar neturintys nuomonės.

Siekiant nustatyti respondentų nuomonę, dėl biometrinių technologijų naudojimo viešojoje erdvėje, apklausoje buvo pateiktas klausimas „Kokia Jūsų pozicija, dėl biometrinių technologijų naudojimo viešojoje erdvėje (pvz., viešojo transporto stotyse, oro uostuose, prekybos centruose)?“ (žr. 20 pav.).



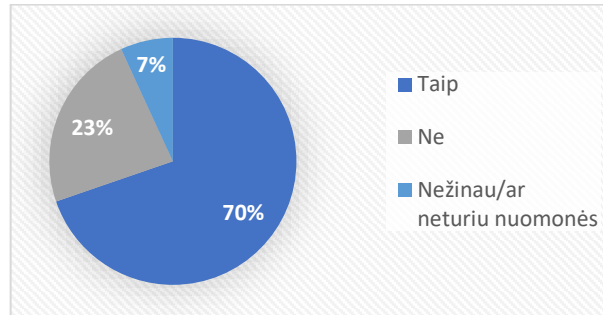
Šaltinis: parengtas autoriaus

20 pav. Biometrinių technologijų naudojimas viešojoje erdvėje

Iš rezultatų matome, jog biometrinių technologijų naudojimas viešojoje erdvėje, didžiajai daliai respondentų yra nepriimtinas, net 45 proc. (98 respondentai) nurodė visiškai nesutinkantys su šių technologijų naudojimu viešojoje erdvėje. Kiek mažesnė dalis, 34 proc. (74 respondentai) nurodė, iš dalies sutinkantys, jog šios technologijos galėtų būti naudojamos viešojoje erdvėje. Dalinai

nesutinkančių nuomonę sudarė, 13 proc. (28 respondentai) apklaustųjų, o likusi dalis 8 proc. (18 respondentų) prieštaravo bet kokiam šių technologijų naudojimui viešojoje erdvėje.

Siekiant nustatyti respondentų nuomonę, dėl informacijos ir švietimo poreikio biometrinių technologijų naudojimo kontekste, apklausoje buvo pateiktas klausimas „Ar manote, kad viešojoje erdvėje reikia daugiau informacijos apie biometrinių technologijų naudojimą, jų poveikį asmens duomenų apsaugai ir kad švietimas šioje srityje turėtų būti didinamas?“ (žr. 21 pav.).

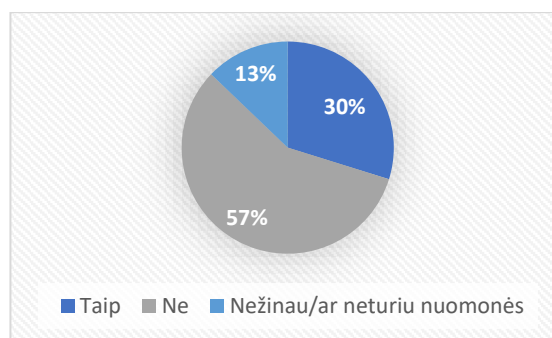


Šaltinis: parengtas autoriaus

21 pav. Informacijos ir švietimo poreikis biometrinių technologijų naudojimo kontekste

Iš gautų rezultatų matome, jog daugiau nei pusę apklaustųjų sutinka, jog yra reikalingas didesnis dėmesys informacijos sklaidos ir švietimo klausimu apie biometrines technologijas, už tai pasisakė 70 proc. (152 respondentai). Kaip tokio poreikio nematantys, nuomonę pareiškė 23 proc. (51 respondentas) apklaustųjų, likę 7 proc. (15 respondentų), nurodė nežinantys ar neturintys nuomonės.

Siekiant nustatyti respondentų nuomonę, ar didesnių įkainių taikymas vartotojams, galėtų užtikrinti didesnę biometrinių technologijų saugumo lygį ir būtų priimtinas. Apklausoje buvo pateiktas klausimas „Ar būtumėte pasirengę mokėti daugiau už produktą ar paslaugą, naudojančią saugesnes biometrines technologijas?“ (žr. 22 pav.).



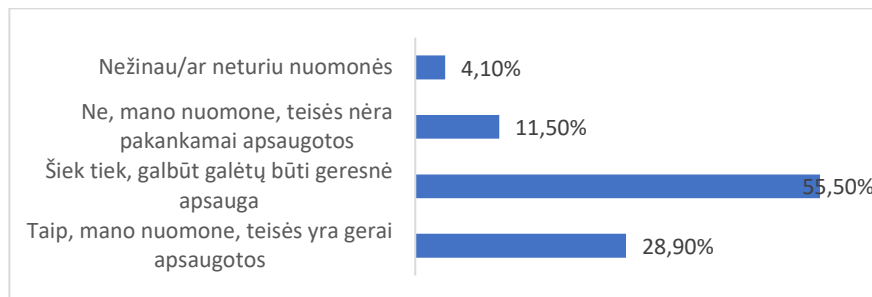
Šaltinis: parengtas autoriaus

22 pav. Nuomonė, dėl didesnių įkainių taikymo produktams ar paslaugoms, naudojančioms saugesnes biometrines technologijas

Rezultatai parodė, jog šiek tiek daugiau nei pusė apklaustųjų, 57 proc. (125 respondentai) nebūtų pasirengę mokėti daugiau už produktą ar paslaugą, naudojančią saugesnes biometrines technologijas. Tačiau atsakiusių tarpe, net 30 proc. (65 respondantai) teigė už tokius produktus ar paslaugas

naudojančias biometrines technologijas, būtų pasiryžę sumokėti daugiau. Maža dalis, 13 proc. (28 respondentai) teigė nežinantys ar neturintys nuomonės, dėl didesnių įkainių taikymo politikos.

Siekiant nustatyti respondentų nuomonę, ar vartotojų teisių apsauga biometrinių technologijų naudojimo srityje yra pakankama, apklausoje buvo pateiktas klausimas „Ar manote, kad vartotojų teisės yra pakankamai apsaugotos biometrinių technologijų naudojimo srityje?“ (žr. 23 pav.).



Šaltinis: parengtas autoriaus

23 pav. Vartotojų teisių apsauga biometrinių technologijų naudojimo srityje

Iš rezultatų matome, kad didžioji dalis apklaustųjų mano, jog vartotojų teisių apsauga biometrinių technologijų naudojimo srityje galėtų būti šiek tiek geresnė, tai pažymėjo 55,50 proc. (121 respondentas). Mažesnę dalis, per 28,90 proc. (63 respondantai) pažymėjo manantys, jog vartotojų teisės yra tinkamai apsaugotos ir jų gerinti poreikio nėra. Likusi dalis, 11,50 proc. (25 respondantai) mano, jog vartotojų teisės nėra tinkamai apsaugotos ir pokyčiai yra reikalingi, 4,10 proc. (9 respondantai) teigia šiuo klausimu neturintys nuomonės arba nežinantys konkretaus atsakymo.

Siekiant įvertinti respondentų pasitenkinimo lygį naudojantis biometrinėmis technologijomis, apklausoje buvo pateiktas klausimas „Ar esate patenkintas dabartiniu biometrinių technologijų lygiu, siekiant apsaugant savo asmeninius duomenis?“ (žr. 24 pav.).



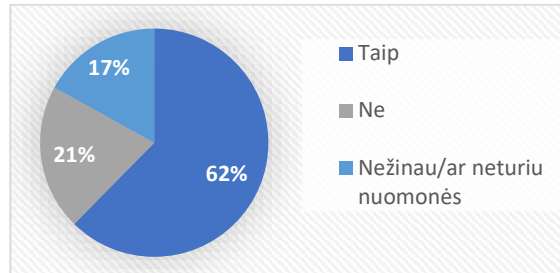
Šaltinis: parengtas autoriaus

24 pav. Pasitenkinimo lygis naudojantis biometrinėmis technologijomis

Iš rezultatų matome, kad 21 proc. (46 respondantai) atsakiusių yra labai patenkinti naudojamomis biometrinėmis technologijomis, kiek daugiau, 31 proc. (67 respondantai) yra tik šiek tiek patenkinti. Likusi dalis respondentų, 21 proc. (46 respondantai) iš dalies yra šiek tiek nepatenkinti

biometrinėmis technologijomis, o 16 proc. (35 respondentai) šiuo klausimu yra neutralios nuomonės. Labai nepatenkintų šių technologijų naudojimusi atsakiusių kiekis sudarė, 11 proc. (24 respondentai).

Siekiant įvertinti respondentų susirūpinimą, dėl biometrinių duomenų perdavimo trečiosioms šalims galimybių, apklausoje buvo pateiktas klausimas „Ar jums kelia nerimą galimybė, kad jūsų biometriniai duomenys gali būti perduoti trečiosioms šalims?“ (žr. 25 pav.).

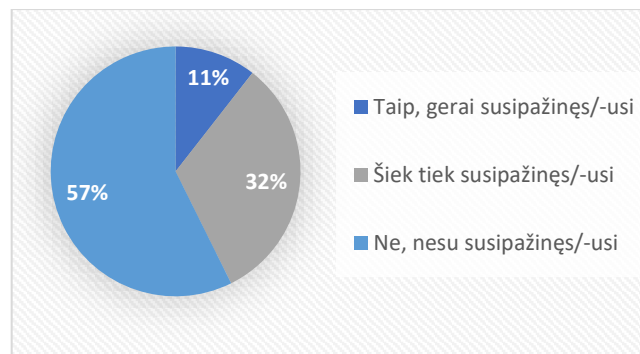


Šaltinis: parengtas autoriaus

25 pav. Nerimas, dėl galimybių biometrinius duomenis perduoti trečiosioms šalims

Iš rezultatų matoma, kad didžioji dalis respondentų, per 62 proc. (136 respondentai) jaučia nerimą, dėl biometrinių duomenų perdavimo trečiosioms šalims galimybių. Maža dalis apklausos dalyvių, per 21 proc. (45 respondentai), mano, kad tokių galimybių tikimybė yra nereikšminga, o likusi dalis 17 proc. (37 respondentai) teigia nežinantys ar neturintys nuomonės.

Siekiant įvertinti respondentų turimas žinias ir susipažinimą su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą, apklausoje buvo pateiktas klausimas „Ar esate susipažinęs/-usi su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą?“ (žr. 26 pav.).



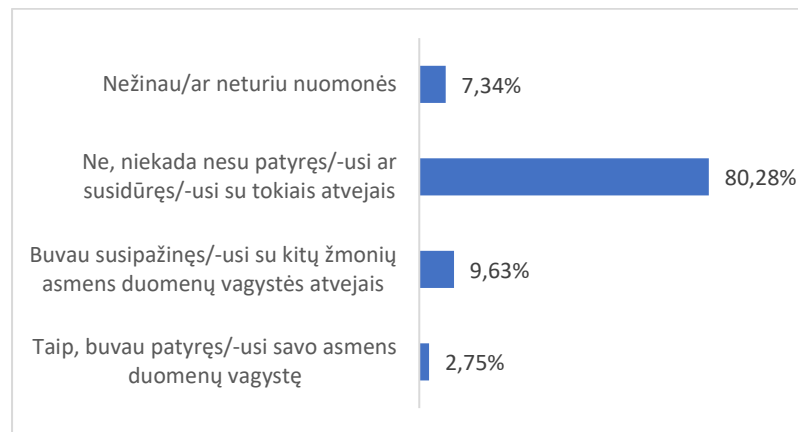
Šaltinis: parengtas autoriaus

26 pav. Susipažinimas su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą

Iš gautų rezultatų matome, jog didžioji dalis nėra gerai susipažinusi su Lietuvoje ir Europos Sąjungoje esamais teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą, tai sudarė 57 proc. (125 respondentai) apklaustųjų. Šiek tiek susipažinusių ar žinančių teisinį reglamentavimą,

sudarė 32 proc. (70 respondentų) apklaustųjų. Labai maža dalis, 11 proc. (23 respondentai) nurodė šiuo klausimu esantys pakankamai gerai susipažinę.

Apklausoje taip pat buvo siekiama nustatyti, ar respondentų tarpe buvo susidurta su asmens duomenų vagystės atvejais. Kas padėtų sudaryti nuomonę ar šie atvejai galėjo paveikti pasitikėjimą biometrinių technologijų naudojimo perspektyvoje. Apklausoje buvo pateiktas klausimas „Ar kada nors patyrėte savo asmens duomenų vagystę arba buvote susipažinęs/-usi su atvejais, kai buvo pavogti kiti žmonių asmens duomenys?“ (žr. 27 pav.).

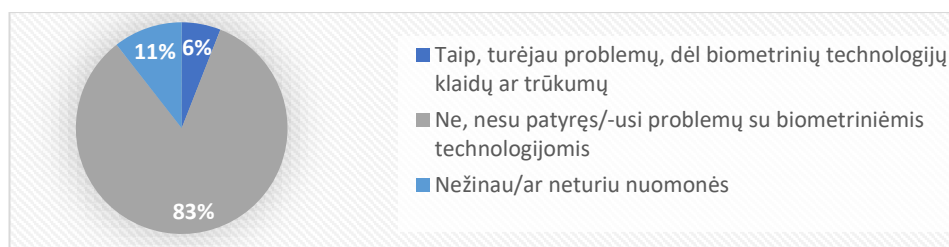


Šaltinis: parengtas autoriaus

27 pav. Susidūrimas su asmens duomenų vagystės atvejais

Iš rezultatų matome, kad susidūrusių su asmens duomenų vagystės atvejais respondentų skaičius yra labai mažas, net 80,28 proc. (175 respondentai) atsakiusių su tokiais atvejais nesusidūrė. Maža dalis, 9,63 proc. (21 respondentas) nurodė, apie tokius atvejus susipažinę iš kitų žmonių atvejų, o 7,34 proc. (16 respondentų) teigė šiuo klausimu neturintys nuomonės arba nežinantys konkretaus atsakymo. Iš visų apklausoje dalyvavusių respondentų, vis tik atsirado maža dalis, 2,75 proc. (6 respondentai), kurie nurodė susidūrę su savo asmens duomenų vagyste.

Galiausiai apklausoje, buvo siekiama nustatyti klaidų ir trūkumų atvejų pasitaikymą respondentų tarpe, naudojantis biometrinėmis technologijomis. Apklausoje buvo pateiktas klausimas „Ar yra tekę susidurti su biometrinių technologijų klaidomis ar trūkumų atvejais atpažįstant asmens tapatybę?“ (žr. 28 pav.).



Šaltinis: parengtas autoriaus

28 pav. Susidūrimas su biometrinių technologijų klaidomis ar trūkumų atvejais

Iš rezultatų matome, jog 83 proc. (182 respondentai) atsakiusieji nesusidūrė su jokiais biometrinių technologijų klaidomis, ar trūkumais atpažįstant asmens tapatybę. Labai maža dalis, 6 proc. (13 respondentų) pažymėjo, turėję problemų su šių technologijų naudojimu, o 11 proc. (23 respondentai, nurodė apie tokius atvejus nežinantys, ar neturintys nuomonės.

Tyrimo išvados:

- Tyrimas parodė, kad didžioji dalis Lietuvos gyventojų nėra gerai susipažinę su biometrinėmis technologijomis, tačiau jomis naudojami per 95 proc. apklaustųjų;
- Tyrimo metu išryškėjo švietimo poreikis biometrinių technologijų naudojimo ir poveikio kontekste;
- Tyrimo metu pastebėta tendencija, kad populiariausios biometrinės technologijos gyventojų tarpe yra pirštų ir veido atpažinimo;
- Tyrimas patvirtino, kad gyventojai supranta galimas pagrindines rizikas, technologijų įtakojamus iššūkius ir grėsmes naudojantis biometrinėmis technologijomis;
- Tyrimas patvirtino, kad gyventojams yra svarbu kaip saugomi ir tvarkomi jų biometriniai duomenys;
- Tyrimo metu nustatytas didžiosios dalies apklausoje dalyvavusių gyventojų prieštaravimas biometrinių technologijų naudojimui viešojoje erdvėje;
- Tyrimas parodė, kad gyventojų nuomone vartotojų teisės nėra pakankamai apsaugotos ir galėtų turėti geresnę apsaugą biometrinių technologijų naudojimo kontekste;
- Tyrimas patvirtino, kad didžioji dalis, 57 proc. gyventojų nėra susipažinę su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą;
- Tyrimas patvirtino gyventojų nepasitikėjimą įmonių naudojančių biometrinės technologijas, tinkamu asmens duomenų saugojimu.

4.7. Biometrinių technologijų plėtros atsparumo grėsmėms modelis, atsižvelgiant į tyrimo rezultatus

Atsparumo modelis sudarytas remiantis tyrimo metu gautomis ekspertų išvadomis ir pastebėjimais, taip pat gyventojų apklausos rezultatais. Šis metodų derinys suteikė galimybes įvertinti techninius ir socialinius biometrinių technologijų naudojimo aspektus, kurie yra svarbūs formuojant atsparumo asmens duomenų apsaugai Lietuvoje modelį. Biometrinių technologijų plėtros grėsmių atsparumo asmens duomenų apsaugai modelis, skirtas užtikrinti, kad biometrinės technologijos būtų naudojamos atsakingai ir nepažeidžiant asmens privatumo teisių. Modelis apima įvairius aspektus, įskaitant teisės aktų tobulinimą, asmens duomenų privatumo apsaugą, švietimo vartotojams skatinimą ir bendradarbiavimą tarp valstybės, privataus sektoriaus, mokslo įstaigų bei vartotojų (žr. 2 lent.).

2 lentelė. Biometrinių technologijų plėtros grėsmių atsparumo asmens duomenų apsaugai Lietuvoje modelis

Aspektas	Veiksmai ir iniciatyvos
Teisės aktų tobulinimas	Esamų teisės aktų atnaujinimas ir peržiūra, naujų teisės aktų reglamentuojančių biometrinių technologijų naudojimą kūrimas.
Asmens duomenų privatumo apsauga	Duomenų šifravimas, anonimizavimas, pseudonimizavimas, bendradarbiavimas tarp mokslo įstaigų ir privataus sektoriaus.
Vartotojų švietimas	Informavimo, švietimo kampanijos orientuotos į vartotojų teisių ir atsakomybių aiškinimą.
Bendradarbiavimas	Valstybinių institucijų, privataus sektoriaus, mokslo įstaigų ir vartotojų partnerystė, bendrų tyrimų vykdymas, plėtros projektai.

Šaltinis: parengtas autoriaus

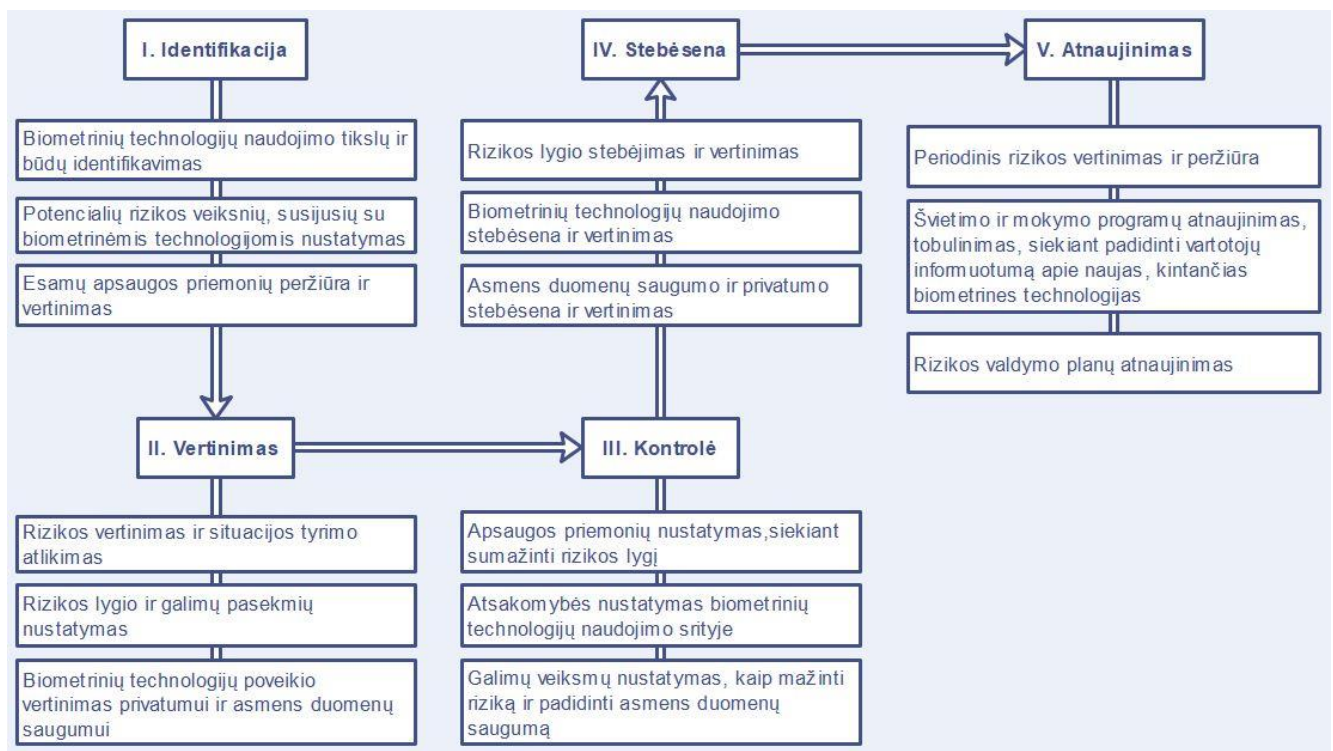
Pirmasis aspektas pateiktas modelyje, teisės aktų tobulinimas, orientuotas į poreikį valstybinėms institucijoms peržiūrėti ir atnaujinti esamus teisės aktus, reglamentuojančius biometrinių technologijų naudojimą, siekiant užtikrinti tinkamą asmens duomenų apsaugą. Tai apima asmens duomenų apsaugos teisės aktų nuostatų atnaujinimą, susijusį su biometriniais duomenimis, taip pat naujų teisės aktų kūrimą, siekiant užtikrinti geresnę privatumo apsaugą. Antrajame aspekte akcentuojamas bendradarbiavimo poreikis tarp privataus sektoriaus ir mokslo įstaigų. Kuriant ir plėtojant pažangias privatumo apsaugos technologijas biometrinėms technologijoms, kaip duomenų šifravimas, anonimizavimas, bei pseudonimizavimas. Šios aspektų metodikos taikymas padės užkirsti kelią neleistinam asmens duomenų naudojimui ir duomenų nutekėjimui taip didinant asmens duomenų privatumo apsaugą. Trečiajame aspekte, akcentuojamas švietimo poreikis vartotojams. Valstybinės institucijos, kartu su privačiu sektoriumi, turėtų vykdyti informavimo, bei švietimo kampanijas, skirtas šviesti vartotojus apie biometrinių technologijų naudojimo rizikas, teises ir atsakomybes. Vartotojai turėtų būti informuoti apie galimus privatumo pažeidimus ir būdus, kaip apsaugoti savo asmens duomenis. Ketvirtasis aspektas akcentuoja bendradarbiavimo poreikį tarp valstybės, privataus sektoriaus, mokslo įstaigų ir pačių vartotojų. Siekiant užtikrinti efektyvų asmens duomenų apsaugos modelį, reikalingas didesnis suinteresuotų šalių tarpusavio bendradarbiavimas. Taikant abipusį bendradarbiavimą, siekiant užtikrinti asmens duomenų apsaugą ir atsparumą grėsmėms, susijusioms su biometrinėmis technologijomis. Kuris apimtų bendrų tyrimų ir plėtros projektų vykdymą, bendrą politikos formavimą, privatumo apsaugos standartų kūrimą, ar informacijos bei geriausių praktikų keitimąsi.

Įgyvendinus šį modelį, Lietuva galėtų užtikrinti estiškesnį, bei atsakingesnį biometrinių technologijų naudojamą, taip pat apsaugoti gyventojų asmens duomenis ir privatumą. Tačiau svarbu

suprasti, jog šis modelis nėra vienintelis sprendimas. Pastovi technologijų plėtra, neišvengiamai iškels papildomas rizikas, bei poreikius modelio tolimesniam tobulinimui ir papildymui.

Biometrinių technologijų plėtra Lietuvoje atveria naujas galimybes įvairiose srityse, tačiau aišku ir tai, kad iš viso to kyla nauji iššūkiai, bei galimos rizikos, susijusios su asmens duomenų apsauga. Tinkamam rizikų valdymui, reikalingas asmens duomenų apsaugos užtikrinimas, o tam būtina sudaryti rizikos valdymo priemonių modelį, atsižvelgiant į Lietuvos teisinę sistemą, technologinę infrastruktūrą, bei gyventojų poreikius ir lūkesčius. Siekiant efektyviau spręsti kylančias problemas ir galimas grėsmes, rizikos valdymo priemonių modelis turi apimti tiek teisinius aspektus, tiek technologines inovacijas, bei švietimą. Modelis bus grindžiamas tyrimo metu gautais rezultatais, įskaitant pateiktą ekspertų nuomonę ir išvalgas, taip pat iš vartotojų apklausos metu surinkta nuomone, požiūriu į biometrines technologijas. Iš tyrimo metu surinktos informacijos, galima teigti, jog Lietuvoje, biometrinių technologijų naudojimo kontekste reikalingas papildomas dėmesys, vartotojų švietimui, teisinio reguliavimo gerinimui, asmens duomenų privatumo užtikrinimui, viešojo sektoriaus naudojančio biometrines technologijas skaidrumo didinimui ir duomenų vagysčių, bei sukčiavimo atvejų mažinimui. Todėl remiantis gautais tyrimo rezultatais, galima geriau suprasti Lietuvoje esamą situaciją ir atsižvelgiant į tai suformuoti tinkamą strategiją rizikos valdymui.

Biometrinių technologijų Lietuvoje rizikos valdymo priemonių modelį viso sudaro penki etapai. Kiekviename modelio etape detalizuojami reikalingi veiksmai, sėkmingam galimų rizikų valdymui įgyvendinti (žr. 29 pav.).



Šaltinis: parengtas autoriaus

29 pav. Rizikos valdymo priemonių modelis

Remiantis sudarytu rizikos valdymo priemonių modeliu, organizacijos ir privatūs asmenys, galės identifikuoti, vertinti ir kontroliuoti biometrinių technologijų naudojimo riziką, asmens duomenų saugumui, bei privatumui. Modelis suteiks galimybes nustatyti reikiamus ir būtinus veiksmus, siekiant sumažinti galimų rizikų atvejus, taip pat užtikrinti asmens duomenų saugumą ir privatumą. Rizikos valdymo priemonių modelį sudaro penki etapai:

- **identifikacija** – identifikavimas galimų rizikos veiksnių, susijusių su biometrinėmis technologijomis, jų poveikiu asmens duomenų saugumui ir privatumui.
- **vertinimas** – nustatymas galimų pasekmių ir rizikų vertinimas, susijusių su biometrinėmis technologijomis ir asmens duomenų saugumu, bei privatumu.
- **kontrolė** – tinkamų rizikos mažinimo priemonių parinkimas, siekiant sumažinti rizikos lygį ir apsaugoti asmens duomenis, bei privatumą.
- **stebėseną** – stebėjimas, vertinimas biometrinių technologijų ir asmens duomenų saugumo situacijos, siekiant laiku įsikišti ir imtis būtinų priemonių, apsaugoti asmens duomenis.
- **atnaujinimas** – rizikos valdymo plano ir priemonių savalaikis atnaujinimas, kad jos atitiktų naujas ir kintančias biometrinių technologijų, bei asmens duomenų saugumo rekomendacijas ir reikalavimus.

IŠVADOS IR REKOMENDACIJOS

1. Biometrinių technologijų samprata ir koncepcija yra išsamiai išnagrinėtos, išskiriant veikimo principus ir taikymo metodikas. Tai padeda suprasti, biometrinių technologijų naudojimo įtakojamus skirtumus, lyginant su įprastais tradiciniais autentifikavimo metodais, įvertinti turimus pranašumus ir trūkumus. Taip pat suprasti šių technologijų veikimo skirtumus, patogumą vartotojui, turimas charakteristikas, tikslumo ir klaidingumo tikimybių atvejų svarbą. Tačiau neteisėti biometrinių duomenų rinkimo ir privatumo pažeidimo atvejai, parodo nepakankamą saugumo lygio užtikrinimą, bei vartotojų švietimą technologijų naudojimo atžvilgiu.
2. Išanalizavus biometrinių technologijų sąlygojamas grėsmes ir pagrindines grėsmių sritis, galima išskirti šešias pagrindines problemas. Kurias sudaro, biometrinių duomenų saugumo pažeidimai, piktnaudžiavimo biometriniais duomenimis atvejai, netikslių duomenų tikimybė, teisinio reguliavimo stoka, pažeidžiamumai kibernetinių atakų atžvilgiu ir privatumo užtikrinimo stoka. Visa tai parodo, jog technologijų plėtra vykta sparčiau, nei spėjama prisitaikyti iš teisinio reglamentavimo pusės, saugumo mechanizmų diegimo ir kontrolės poreikių.
3. Ištyrus Lietuvos vartotojų požiūrį į biometrines technologijas ir asmens duomenų saugumą. Remiantis tyrimo duomenimis, gyventojai aktyviai naudojami biometrinėmis technologijomis, tačiau nėra gerai susipažinę su pačia technologija ir jos veikimo metodika. Tyrimas parodė, jog gyventojams svarbu kaip saugomi ir tvarkomi jų biometriniai duomenys. Taip pat parodė esantį švietimo trūkumą ir įmonių naudojančių biometrines technologijas nepasitikėjimą. Tyrimo rezultatai atskleidė, kad biometrinių technologijų plėtra ir taikymas viešajame sektoriuje, taip pat kelia didelį gyventojų prieštaravimą, bei nepasitenkinimą.
4. Remiantis atlikta duomenų analize ir ekspertų pateikta nuomone, galima teigti, jog biometrinės technologijos turėtų būti kuriamos iš saugumo, bet ne iš funkcionalumo perspektyvos. Biometrinių duomenų tvarkymas ir saugojimas, sistemose turi atitikti aukščiausius saugumo reikalavimus. Turėtų būti didinamas biometrinių technologijų naudojimo proceso skaidrumas. Kaip galimas problemas, galima išskirti įstatymų neapsaugojimą nuo asmens duomenų rinkimo privačiais tikslais, netinkamą pramonės savireguliaciją, neturinčią įpareigojančių teisės aktų ir tinkamų auditavimo galimybių.

Rekomendacijos:

- reikėtų atsižvelgti į biometrinių technologijų galimybes apsaugoti asmens duomenis ir siūlomą saugumo lygį. Biometrinės technologijos turėtų būti naudojamos atsižvelgiant į priimtina patikimumo ir saugumo funkcionalumo santykį.
- siekiant užtikrinti asmens biometrinių duomenų tvarkingą saugojimą, bei apdorojimą, visais atvejais reikėtų pasitelkti papildomų saugumo priemonių naudojimą, kaip duomenų šifravimą ir duomenų atkūrimą.

- svarbu taikyti griežtas asmens duomenų saugumo taisykles ir procedūras, siekiant užtikrinti tinkamą duomenų apsaugos lygį.
- svarbu įdiegti reikiamas papildomas technines priemones, siekiant identifikuoti asmens duomenų neteisėtus prieigos atvejus, taip apsaugant duomenis nuo galimų vagysčių ir kibernetinių atakų rizikos.
- tinkamas taisyklių ir procedūrų savalaikis įgyvendinimas, siekiant užtikrinti reikiamą asmens teisių ir privatumo apsaugą.
- vartotojų informavimas biometrinių duomenų saugumo klausimais. Informacija turėtų būti pateikiama aiškiai ir suprantamai, siekiant padėti priimti sprendimą, dėl biometrinių duomenų naudojimo ar dalinimosi poreikio.
- reguliavimo ir kontrolės priemonių taikymas, siekiant užtikrinti reikiamą biometrinių duomenų apsaugos lygį. Mechanizmai apimantys prieigos prie duomenų kontroliavimą, duomenų apdorojimo taisyklių laikymąsi ir reguliavimo institucijų stebėjimo taikymą.
- įgyvendinant ir vykdant biometrinių technologijų projektus, įtraukti asmens duomenų apsaugos ekspertus, taip siekiant užtikrinti atitinkamą duomenų saugumą, laikantis galiojančių duomenų apsaugos teisės aktų.
- kelių biometrinių priemonių taikymas vienu metu, tapatumo patvirtinimo metu, ar kombinuotas kelių skirtingų autentifikavimo metodų naudojimas, siekiant užtikrinti didesnę apsaugos lygį, taip sumažinant galimas rizikas.
- galimybės, vartotojui peržiūrėti savo saugomus biometrinius duomenis, gauti informaciją apie jų tvarkymą, su galimybe prireikus juos pašalinti.
- susitarimų ir sutarčių sudarymas su biometrinių duomenų tvarkymo paslaugų teikėjais, ar kitomis trečiosiomis šalimis, siekiant užtikrinti tinkamą asmens duomenų apsaugos lygį.
- reguliarius su asmens duomenimis dirbančių darbuotojų informavimas apie duomenų apsaugos reikalavimus, mokymų pagal poreikį taikymas, siekiant didinti atsakomybę atsakingai tvarkyti asmens duomenis.
- savalaikis apsaugos sistemų tobulinimas, atnaujinimas, siekiant užtikrinti biometrinių technologijų atsparumą naujoms kibernetinėms grėsmėms ir atakoms.

LITERATŪRA

1. Abate, A. F., Fenu, G., Marcialis, G. L., & Roli, F. (2018). *Privacy-preserving biometric authentication systems: A survey*. ACM Computing Surveys (CSUR), 51(5), 1-34
2. Abdulmonam, O. A., Ahlhal, H. M., & Fawzia, E. M. (2014). *Vulnerabilities of Biometric Authentication Threats and Countermeasures*. International Journal of Information Technology and Computer Science, 4(10), 1-8. Prieiga per internetą:
https://www.ripublication.com/irph/ijict_spl/ijictv4n10spl_01.pdf
3. Ahmed, E., Khan, S. U., & Ali, M. A. M. (Eds.). (n.d.). *Handbook of Research on Security Considerations in Cloud Computing* (pp. 97-119). Prieiga per internetą: <https://doi.org/10.4018/978-1-7998-5566-9.ch005>
4. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems*. Wiley. Prieiga per internetą:
https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf
5. Anil K. Jain, Arun Ross and Salil Prabhakar, *An Introduction to Biometric Recognition*, proc. IEEE Transactions on circuits and systems for video technology, Vol.14, No. 1, 2004. Prieiga per internetą: https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf.
6. Augustinaitis A., Rudzkienė V., Petrauskas R. ir kt. (2009). *Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas*. Mykolo Romerio universitetas
7. Aware. (2020). *Biometrics-as-a-service (BaaS)*. Prieiga per internetą:
<https://www.aware.com/biometrics-as-a-service/>
8. Bhardwaj, A., Jain, R., Gupta, V., & Goyal, M. (2020). *Biometric secured financial transactions using near-infrared hand vein pattern recognition*. Journal of Ambient Intelligence and Humanized Computing, 11, 1765–1773
9. Bhatnagar, A., & Jain, A. K. (2019). *Privacy issues in biometric systems: A comprehensive survey*. ACM Computing Surveys (CSUR), 52(5), 1-38
10. Biometrics Institute. (2019). *Biometrics Institute Industry Survey 2019 report*. Prieiga per internetą:
<https://www.biometricsinstitute.org/wp-content/uploads/2019/11/Biometrics-Institute-Industry-Survey-2019-Report-Final.pdf>
11. Bolle, R. (2006). *Biometrics: Personal identification in networked society*. Springer
12. Bond, C., Hassouna, M. S., & Buford, J. (2015). *An exploratory study of smartphone fingerprint recognition technology*. Journal of Information Security and Applications, 20, 1-8
13. California Legislative Information. (2018). *California Consumer Privacy Act of 2018*. Prieiga per internetą: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

14. CNA Hardy. (n.d.). *Cyber security: The future risk of biometric data theft*. Prieiga per internetą: <https://www.cnahardy.com/news-and-insight/insights/english/cyber-security-the-future-risk-of-biometric-data-theft>
15. Campbell, A. (2021). *Suprema hack: Biometric security firm data breach affects 1 million people*. Prieiga per internetą: <https://www.zdnet.com/article/suprema-hack-biometric-security-firm-data-breach-affects-1-million-people/>
16. Chen, S., Chen, C., Wang, W., & Yang, Y. (2020). *A secure mobile authentication mechanism using voice biometrics*. *Mobile Information Systems*, 2020, 1-10
17. Chhabra, G., & Narayanan, A. (2013). *Reducing Cyber Threats: via a Multimodal Biometric System*. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(6), 876-880. Prieiga per internetą: https://www.researchgate.net/publication/280057261_Reducing_Cyber_Threats_via_a_Multimodal_Biometric_System
18. Cisco. (2019). *GDPR compliance: Six months later*. Prieiga per internetą: https://www.cisco.com/c/dam/m/en_uk/collateral/white-papers/gdpr-compliance-six-months-later.pdf
19. Comparitech. (n.d.). *Apie mus*. Prieiga per internetą: <https://www.comparitech.com/about-us/>
20. Damer, N. (2021). *Biometric security: Issues and challenges*. In *The Handbook of Information Security* (pp. 1-20). Wiley. Prieiga per internetą: <https://doi.org/10.1002/9781119643903.ch1>
21. Diaz, J. (2021, June 17). *Canon's new AI camera can recognize when office workers aren't wearing masks — and even check their smiles*. Prieiga per internetą: <https://www.theverge.com/2021/6/17/22538160/ai-camera-smile-recognition-office-workers-china-canon>
22. Dikčius, V. (2016). *Anketos sudarymo principai*. Prieiga per internetą: https://www.academia.edu/29780033/ANKETOS_SUDARYMO_PRINCIPAI
23. Doe, J. (2022). *Biometrics and Cybersecurity: Enhancing Security in the Digital Age*. *Journal of Cybersecurity*, 10(1), 35-48. Prieiga per internetą: <https://doi.org/10.1093/cybsec/tyab001>
24. European Commission. (2016). *General Data Protection Regulation*. Prieiga per internetą: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
25. Fang, B., Yang, Y., Zhang, D., Xu, X., & Yan, J. (2019). *Finger-vein recognition using a smartphone camera and near-infrared light*. *Journal of Electronic Imaging*, 28(5), 053015
26. Faulkner, C. (2017). *What is NFC?*. Prieiga per internetą: <https://www.techradar.com/news/what-is-nfc>
27. FIDO Alliance. (2020). *FIDO2*. Prieiga per internetą: <https://fidoalliance.org/fido2/>
28. Gao, H., Li, M., Chen, X., & Chen, M. (2019). *An implantable and subdermally injectable RFID system for animal identification and tracking*. *IEEE Transactions on Industrial Electronics*, 66(3), 2097-2106

29. Ghatak, A., & Ray, P. (2019). *A review on human chip implantation technology*. International Journal of Emerging Trends & Technology in Computer Science, 8(5), 43-46
30. Grand View Research. (2021). *Facial Recognition Market Size, Share & Trends Analysis Report By Application (Emotion Recognition, Attendance Tracking), By Technology (2D, 3D, Thermal), By End-use, By Region, And Segment Forecasts, 2020 - 2027*. Prieiga per internetą: <https://www.grandviewresearch.com/industry-analysis/facial-recognition-market>
31. Gupta, P., & Gupta, P. (2017). *A survey on biometrics and cancelable biometrics systems*. Journal of Network Communications and Emerging Technologies, 7(4), 43-57
32. Hoffman, C. (2016). *What is RFID, and is it really a security concern?* Prieiga per internetą: <https://www.howtogeek.com/179468/what-is-rfid-and-is-it-really-a-security-concern/>
33. Human Rights Watch. (2020). *China: Facial Recognition System A Threat to Privacy*. Human Rights Watch. Prieiga per internetą: <https://www.hrw.org/news/2020/01/15/china-facial-recognition-system-threat-privacy>
34. iProov. (2021). *Deepfakes and Biometric Security: The impact of synthetic media on biometric authentication*. Prieiga per internetą: <https://www.iproov.com/wp-content/uploads/2021/05/iProov-Deepfakes-Report.pdf>.
35. Islam, M. S., Hoque, M. M., & Wang, H. (2021). *Voice recognition and deepfake detection for security applications*. SN Computer Science, 2(4), 1-12
36. International Organization for Standardization/International Electrotechnical Commission. (2011). *ISO/IEC 19794-1: Information technology - Biometric data interchange formats - Part 1: Framework*
37. International Organization for Standardization/International Electrotechnical Commission. (2016). *ISO/IEC 30107-1: Information technology - Biometric presentation attack detection - Part 1: Framework*
38. Jain, A. K., & Ross, A. (2020). *Introduction to biometrics*. Springer
39. Jain, A. K., & Ross, A. (2020). *The efficiency and cost-effectiveness of iris recognition technology in large corporations*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 3813-3820)
40. Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to biometrics*. Springer
41. Joseph M., Michael K., Stephen K. (2019). *A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates*. International Journal of Electronics Engineering: Prieiga per internetą: <https://docplayer.net/139018878-Sakshi-nagpal-m-tech-student-department-of-computer-science-and-application-k-u-kurukshetra-haryana-india.html>
42. Marcel, S., Nixon, M., & Li, S. Z. (2014). *Handbook of Biometric Anti-Spoofing*. Springer

43. Kollwe J. (2018). *Alarm over talks to implant UK employees with microchips*. Prieiga per internetą: <https://www.theguardian.com/technology/2018/nov/11/alarm-over-talks-to-implant-uk-employees-with-microchips>
44. Kumar, H. (2021). *Presentation Attack Detection in Facial Biometric Authentication*. Prieiga per internetą: https://scholarworks.sjsu.edu/etd_projects/1002
45. Latha U. ir Rameshkumar K. A. (2013). *Study on Attacks and Security Against Fingerprint Template Database*. Prieiga per internetą: <https://www.ijettcs.org/Volume2Issue5/IJETTCS-2013-08-05-017.pdf>
46. Leedy, P. D., & Ormrod, J. E. (2020). *Practical research: Planning and design* (12th ed.). Pearson
47. Li, Z., Huang, Y., & Jain, A. K. (2019). *A survey of deep learning-based biometric recognition*. ACM Computing Surveys, 52(4), 67. Prieiga per internetą: <https://doi.org/10.1145/3316936>
48. Ma, A. (2018). *Thousands of people in Sweden are embedding microchips under their skin to replace ID cards*. Prieiga per internetą: <https://www.businessinsider.com.au/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=us&ir=t>
49. Marasco, E., & Ross, A. (2015). *A survey on antispooofing schemes for fingerprint recognition systems*. ACM Computing Surveys, 47(2), A:1-A:36. doi: 10.1145/2701415
50. MarketsandMarkets. (2022). *Biometric Technology Market by Authentication Type, Component, Functionality, Deployment, Organization Size, Vertical And Region - Global Forecast to 2026*. Prieiga per internetą: <https://www.marketsandmarkets.com/Market-Reports/biometric-technology-market-697.html>
51. Mastercard. (2021). *Mastercard Launches First-ever Biometric Card in Asia Pacific to Simplify and Secure Transactions*. Prieiga per internetą: <https://www.mastercard.com/news/asia-pacific/en/newsroom/press-releases/en/2021/april/mastercard-launches-first-ever-biometric-card-in-asia-pacific-to-simplify-and-secure-transactions/>
52. Mauro, A. (2022). *Retina Recognition*. Biometric Technology Today, 2022(1), 1-3. Prieiga per internetą: <https://doi.org/10.1016/j.bite.2022.01.001>
53. Munir, S., & Siddique, M. (2021). *Biometric Data Security: Issues, Challenges, and Solutions*
54. Nandakumar, K., Ross, A., & Jain, A. K. (2016). *Introduction to biometrics*. Springer
55. National Research Council. (2010). *Biometric recognition: Challenges and opportunities*. National Academies Press. Prieiga per internetą: <https://doi.org/10.17226/12720>
56. NIST SP 800-63B. (2017). *Digital identity guidelines*
57. NIST SP 800-76. (2013). *Biometric data specification for personal identity verification*
58. Pagnin E., Dimitrakakis C., Abidin A. ir Mitrokovtsa A. *On the leakage of information in biometric authentication*. Prieiga per internetą: <https://portal.research.lu.se/en/publications/on-the-leakage-of-information-in-biometric-authentication>

59. Ragazzi, F., Kuskonmaz, E. M., Plájás, I. Z., van de Ven, R., & Wagner, B. (2021). *Biometric surveillance technologies: The urgent need for a solid EU regulatory framework*. Europos Parlamento Žaliųjų/EFA frakcija. Prieiga per internetą: <https://www.greens-efa.eu/biometricsurveillance/>
60. ResearchAndMarkets. (2021). *Biometric Wearables Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)*. Prieiga per internetą: <https://www.researchandmarkets.com/reports/5313584/biometric-wearables-market-growth-trends-covid>
61. Rhue L. (2018). *Racial influence on automated perceptions of emotions*. College Park, University of Maryland. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765
62. Ross, A., & Jain, A. K. (2015). *Handbook of biometrics*. Springer
63. Ross, A., Nandakumar, K., & Jain, A. K. (2017). *Handbook of biometrics*. Springer
64. Ross, A., Nandakumar, K., & Jain, A. K. (2021). *Handbook of biometrics*. Springer
65. Ross, A., Nandakumar, K., & Jain, A. K. (2021). *Performance evaluation of iris recognition technology*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 5269-5277)
66. Yoon, S., Feng, J., & Jain, A. K. (2012). *Altered fingerprints: Analysis and detection*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 34(3), 451-464
67. Sydney Morning Herald. (2003). *The print that never fades*. Prieiga per internetą: <https://www.smh.com.au/national/the-print-that-never-fades-20031127-gdhv4w.html>
68. Singh S. (2018). *Understanding Aadhaar: The unique identification authority of India and its challenges*. Human Rights Defender 27 (3): 21–24
69. Smith, J. (2020). *Global Privacy Trends and the GDPR: Where Are We Now?* Prieiga per internetą: <https://www.forbes.com/sites/forbestechcouncil/2020/01/27/global-privacy-trends-and-the-gdpr-where-are-we-now/?sh=26da1a3a3d99>
70. Tota, I. A., Bajčetić, J. B., Jovanović, B. Ž., Trikoš, M. B., Bogićević, D. Lj., & Gajić, T. M. (2019). *Biometric standards and methods*. Facta Universitatis, Series: Electronics and Energetics, 32(2), 223-242
71. TrustArc. (2020). *CCPA compliance: A year later*. Prieiga per internetą: <https://www.trustarc.com/resource/ccpa-compliance-a-year-later/>

Sriubas E. (2023). *Biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuota biometrinių technologijų plėtros grėsmės ir daroma įtaka asmens duomenų apsaugai. Pirmame darbo skyriuje nagrinėja biometrinių technologijų sampratą, veikimo principai, plėtros tendencijos, sąlygojamos grėsmės, galimos atakos. Taip pat asmens duomenų apsaugos reglamentavimą, biometrikos ir kibernetinio saugumo standartai. Antrame skyriuje analizuojami tarptautiniai ir ES kontekste atlikti tyrimai, susiję su biometrinių technologijų naudojimo įtakojamomis problemomis. Trečiame skyriuje pristatoma Lietuvos vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą tyrimo metodologija. Ketvirtame skyriuje pateikiami empirinio tyrimo rezultatai, apimantys biometrinių technologijų įtaką asmens duomenų saugumui ir privatumui, etines problemas, susijusias su biometrikos naudojimu, vartotojų švietimo ir informuotumo didinimo kampanijų svarbą, pramonės savireguliacijos vaidmenį, bei biometrinių technologijų ateitį. Skyriuje taip pat, pateikiami Lietuvos vartotojų požiūrio į biometrines technologijas ir asmens duomenų saugumą tyrimo rezultatai. Atsižvelgiant į tyrimo rezultatus pateikiamas biometrinių technologijų plėtros atsparumo grėsmėms modelis. Penktajame skyriuje pateikiamos išvados ir rekomendacijos atsparumo didinimui, biometrinių technologijų sąlygojamoms grėsmėms.

Pagrindiniai žodžiai: biometrinės technologijos, asmens duomenų apsauga, grėsmės, privatumas, plėtra.

Sriubas E. (2023). *Threats of the development of biometric technologies for the protection of personal data* (master thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The Master's thesis analyses the threats and impact of the development of biometric technologies on the protection of personal data. The first chapter of the thesis deals with the concept of biometric technologies, principles of operation, development trends, threats and possible attacks. It also covers the regulation of personal data protection, biometrics and cybersecurity standards. The second chapter analyses international and EU research on the issues affected by the use of biometric technologies. The third chapter presents the methodology of the study on the attitude of Lithuanian consumers towards biometric technologies and personal data security. Chapter four presents the results of the empirical research, covering the impact of biometric technologies on personal data security and privacy, ethical issues related to the use of biometrics, the importance of consumer education and awareness campaigns, the role of industry self-regulation, and the future of biometric technologies. The chapter also presents the results of a survey on the attitudes of Lithuanian consumers towards biometric technologies and personal data security. In the light of the survey results, a threat resilience model for the development of biometric technologies is presented. The fifth chapter presents conclusions and recommendations for improving resilience to threats posed by biometric technologies.

Key words: biometric technologies, personal data protection, threats, privacy, development.

Sriubas E. (2023). *Biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Biometrinės technologijos šiuo metu yra aktuali tema, kuri turi didelę teorinę svarbą šių dienų kontekste, vykstanti technologijų plėtra, atveria terpę potencialioms grėsmėms įtakojančioms asmens duomenų saugumą ir privatumą. Biometriniai duomenys pasižymi unikalumu ir nekintamumu, ko pasėkoje kompromitacijos atveju, atsiranda negrįžtama tam tikrų grėsmių, bei pavojų tikimybė. Tyrimo objektas – biometrinių technologijų taikymas asmens tapatybei nustatyti, plėtros įtakojamos grėsmės asmens duomenų apsaugai. Šio tyrimo tikslas yra išanalizuoti biometrinių technologijų plėtros grėsmes asmens duomenų apsaugai. Taip pat buvo išsikelti ir tyrimo uždaviniai: išnagrinėti biometrinių technologijų sampratą ir koncepciją, išanalizuoti biometrinių technologijų sąlygojamas grėsmes, ištirti Lietuvos vartotojų požiūrį į biometrines technologijas ir asmens duomenų saugumą, sukurti biometrinių technologijų plėtros Lietuvoje atsparumo grėsmėms modelį, pateikti rekomendacijas, kaip užtikrinti biometrinių technologijų plėtros atsparumą grėsmėms asmens duomenų apsaugai, atsižvelgiant į tyrimo rezultatus. Tyrimo metodika: mokslinės literatūros analizė ir sisteminimas, tyrimų apžvalga ir analizė, kokybinė ir kiekybinė duomenų analizė. Šiame darbe išanalizuotos biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai. Darbe apžvelgti teoriniai biometrinių technologijų sampratos aspektai, jų veikimo principai, bei sąlygojamos grėsmės. Aptarti asmens duomenų apsaugos reglamentavimo klausimai, biometrikos ir kibernetinio saugumo standartai. Išanalizuoti ES kontekste atlikti tyrimai. Empiriniame tyrime išanalizuotas Lietuvos vartotojų požiūris į biometrines technologijas ir asmens duomenų saugumą. Tyrimo rezultatai atskleidė vartotojų nuomonę biometrinių technologijų grėsmių atžvilgiu asmens duomenų apsaugai ir privatumui, esančias etines problemas, vartotojų švietimo ir informuotumo didinimo kampanijų reikalingumą, pramonės savireguliacijos vaidmenį, bei biometrinių technologijų ateitį. Remiantis tyrimo rezultatais sudarytas biometrinių technologijų plėtros grėsmių atsparumo asmens duomenų apsaugai Lietuvoje ir rizikos valdymo priemonių modeliai. Darbe pateikiamos išvados ir rekomendacijos, skirtos mažinti biometrinių technologijų plėtros grėsmes asmens duomenų apsaugai.

Sriubas E. (2023). *Threats of the development of biometric technologies for the protection of personal data* (master thesis). Vilnius: Mykolas Romeris University

SUMMARY

Biometric technologies are currently a hot topic that has great theoretical relevance in today's context, as the ongoing development of the technology opens up the field to potential threats affecting the security and privacy of personal data. Biometric data are unique and immutable, which, in the event of a compromise, leads to an irreversible probability of certain threats and risks. The object of the study is the application of biometric technologies for the identification of a person and the threats to the protection of personal data as a result of the development. The aim of this study is to analyse the threats to the protection of personal data caused by the development of biometric technologies. The objectives of the study were also: to analyse the concept and conception of biometric technologies, to analyse the threats caused by biometric technologies, to investigate the attitude of Lithuanian consumers towards biometric technologies and security of personal data, to develop a model of threat resistance of biometric technologies development in Lithuania, to provide recommendations on how to ensure the resistance of biometric technologies development to threats to the protection of personal data in the light of the study results. Research methodology: analysis and systematisation of scientific literature, review and analysis of studies, qualitative and quantitative data analysis. This paper analyses the threats to the protection of personal data posed by the development of biometric technologies. The theoretical aspects of the concept of biometric technologies, their principles of operation, and the resulting threats are reviewed. It discusses the regulatory issues of personal data protection, biometrics and cybersecurity standards. Studies carried out in the EU context are analysed. The empirical study analysed the attitudes of Lithuanian consumers towards biometric technologies and personal data security. The results of the study revealed consumers' views on the threats of biometric technologies to the protection and privacy of personal data, the ethical issues at stake, the need for consumer education and awareness-raising campaigns, the role of industry self-regulation, and the future of biometric technologies. Based on the results of the study, a model of the resilience of biometric technology development to threats to personal data protection in Lithuania and risk management measures was developed. The paper presents conclusions and recommendations to mitigate the threats to the protection of personal data from the development of biometric technologies.

PRIEDAI

Priedas 1. tyrime naudota anketa

Apklauso duomenys bus naudojami Mykolo Romerio universiteto vadybos mokslo krypties, valstybės finansuojamų, išstęstinių magistratūros studijų studento Edgaro Sriubo magistriniame darbe tema „Biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai“.

Dalyvavimas apklausoje yra anoniminis, pateikti atsakymai bus renkami ir analizuojami tiriamajame darbe, atsižvelgiant į duomenų apsaugos ir privatumo reikalavimus.

Apklauso tikslas – sužinoti Jūsų, kaip eksperto nuomonę ir turimą patirtį, dėl biometrinių technologijų naudojimo Lietuvoje užtikrinant asmens duomenų saugumą ir privatumą.

1. Kokią įtaką, jūsų nuomone, biometrinės technologijos daro asmens duomenų saugumui Lietuvoje ir kokia galima šių technologijų rizika ir nauda?

2. Kokios yra aktualiausios etinės problemos, susijusios su biometrinių technologijų naudojimu asmens duomenims rinkti ir tvarkyti, kaip šias problemas galima būtų spręsti?

3. Kaip vertinate dabartinę biometrinių technologijų situaciją Lietuvoje, kokias pagrindines tendencijas ir iššūkius matote šioje srityje?

4. Kokios teisinės ir reguliavimo sistemos šiuo metu Lietuvoje reglamentuoja biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui, kaip manote, kiek veiksmingai šios sistemos apsaugo asmens privatumo teises?

5. Kaip manote, koks vaidmuo gali tekti vartotojų švietimui ir informuotumo didinimo kampanijoms, siekiant informuoti Lietuvos visuomenę apie biometrinių technologijų tinkamą naudojimą, bei sąlygojamas grėsmes, ir kokios strategijos šiuo atžvilgiu būtų veiksmingiausios?

6. Kaip biometrinės technologijos galėtų būti kuriamos ir diegiamos, siekiant užtikrinti didesnę privatumo, bei saugumo lygį, tuo pačiu teikiant naudą vartotojams ir organizacijoms?

7. Kaip būtų galima atnaujinti ar sugriežtinti duomenų apsaugos ir privatumo įstatymus, kad būtų galima spręsti unikalios biometrinių technologijų keliamus iššūkius ir kokie vykdymo užtikrinimo mechanizmai būtų veiksmingiausi šiame kontekste?

8. Kokį vaidmenį, jūsų nuomone, atlieka pramonės savireguliacija skatinant atsakingą biometrinių technologijų naudojimą ir kokios yra pagrindinės veiksmingos savireguliacijos sistemos sudedamosios dalys?

9. Kaip, jūsų nuomone, biometrinių technologijų naudojimas Lietuvoje vystysis artimiausiais metais ir kokį poveikį tai turės asmens duomenų saugumo ir privatumo užtikrinimui?

10. Kokias pasiūlytumėte pagrindines rekomendacijas ar sprendimus, siekiant padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje ir kaip šios rekomendacijos galėtų būti įgyvendintos praktiškai?

Ačiū, kad skyrėte savo laiką ir sudalyvavote apklausoje

Priedas 2. tyrime naudota anketa

Apklauso duomenys bus naudojami Mykolo Romerio universiteto vadybos mokslo krypties, valstybės finansuojamų, išstęstinių magistratūros studijų studento Edgaro Sriubo magistriniame darbe tema „Biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai“.

Dalyvavimas apklausoje yra anoniminis, pateikti atsakymai bus renkami ir analizuojami tiriamajame darbe, atsižvelgiant į duomenų apsaugos ir privatumo reikalavimus.

Apklauso tikslas – ištirti Lietuvos vartotojų požiūrį į biometrines technologijas ir jų įtaką asmens duomenų saugumui, siekiant suformuoti rekomendacijas, kaip padidinti biometrinių technologijų atsparumą asmens duomenų apsaugos grėsmėms Lietuvoje.

1. Kokiai amžiaus grupei priklausote?

- ☐ 18-25 metai
- ☐ 26-35 metai
- ☐ 36-45 metai
- ☐ 46-55 metai
- ☐ 56 metai ar vyresni

2. Koks yra Jūsų išsilavinimas?

- ☐ Pagrindinis išsilavinimas
- ☐ Vidurinis išsilavinimas
- ☐ Profesinis išsilavinimas
- ☐ Aukštasis išsilavinimas
- ☐ Aukštasis išsilavinimas, mokslinis laipsnis

3. Kiek gerai esate susipažinę su biometrinėmis technologijomis?

- ☐ Gerai susipažinęs/-usi
- ☐ Šiek tiek susipažinęs/-usi
- ☐ Šiek tiek girdėjęs/-usi
- ☐ Visiškai nežinau, kas yra biometrinės technologijos

4. Kurias biometrines technologijas jau esate naudoję/-usi savo kasdieninėje veikloje?

- ☐ Pirštų atspaudų skaitymas
- ☐ Veido atpažinimas
- ☐ Balso atpažinimas
- ☐ Akių atpažinimas
- ☐ Širdies ritmo sekimas
- ☐ Naudotis neteko

5. Ar naudojate biometrines technologijas savo įrenginiuose (pvz., išmaniajame telefone ar kompiuteryje)?

- ☐ Taip
- ☐ Ne
- ☐ Nežinau/ar neturiu nuomonės

6. Ar manote, kad biometrinės technologijos yra saugesnės nei tradicinės tapatybės patvirtinimo priemonės (pvz., slaptažodžiai)?

- ☐ Taip
- ☐ Ne
- ☐ Niekada apie tai nesusimasčiau

7. Jei galėtumėte pasirinkti tarp tradicinės tapatybės patvirtinimo priemonės (pvz., slaptažodžio) ir biometrinės technologijos, kurią pasirinktumėte?

- ☐ Pasirinkčiau biometrinę technologiją
- ☐ Pasirinkčiau tradicinę tapatybės patvirtinimo priemonę
- ☐ Nemanau, kad turėčiau pasirinkti

8. Kiek svarbu, kad Jūs turėtumėte kontrolę, dėl savo biometrinių duomenų rinkimo, saugojimo ir naudojimo?

- ☐ Labai svarbu
- ☐ Gana svarbu
- ☐ Nėra itin svarbu
- ☐ Visiškai nesvarbu
- ☐ Nežinau/ar neturiu nuomonės

9. Kokias pagrindines rizikas matote naudojantis biometrinėmis technologijomis asmens duomenų saugumo požiūriu? (atsakymai gali būti pasirinkti daugiau nei vienas)

- ☐ Rizika, kad biometriniai duomenys bus pavogti
- ☐ Rizika, kad biometriniai duomenys bus neteisingai naudojami
- ☐ Rizika, kad asmens duomenys bus nelegaliai perduoti trečiosioms šalims
- ☐ Nemanau, kad biometrinės technologijos yra rizikingos asmens duomenų saugumo požiūriu
- ☐ Nežinau/ar neturiu nuomonės

10. Kokia yra jūsų bendra nuomonė apie biometrinių technologijų naudojimą asmens duomenų rinkimui ir tvarkymui?

- ☐ Labai palanki
- ☐ Šiek tiek palanki
- ☐ Šiek tiek nepalanki
- ☐ Visiškai nepalanki

11. Kokius matote galimus pagrindinius iššūkius ir rizikos veiksnius susijusius su biometrinėmis technologijomis Lietuvoje? (atsakymai gali būti pasirinkti daugiau nei vienas)

- ☐ Reguliavimo trūkumas
- ☐ Netinkamas biometrinių duomenų saugojimas
- ☐ Duomenų vagystė ir sukčiavimas
- ☐ Tikimybė, kad biometriniai duomenys gali būti suklastoti arba pakoreguoti
- ☐ Asmeninių duomenų rinkimo kiekio skaitmeninėje erdvėje didėjimo tendencija
- ☐ Kita

12. Ar manote, kad viešosios institucijos ir privačios įmonės turėtų būti privalomai vertinamos pagal jų asmens duomenų saugumo politiką ir naudojamas biometrines technologijas?

- ☐ Taip
- ☐ Ne

- ☐ Nemanau, kad tai turėtų būti privaloma

13. Kiek Jums svarbu, kad įmonės, kurios naudoja biometrines technologijas, informuotų apie savo asmens duomenų tvarkymo praktikas?

- ☐ Labai svarbu
☐ Gana svarbu
☐ Nėra itin svarbu
☐ Visiškai nesvarbu
☐ Nežinau/ar neturiu nuomonės

14. Ar Jūs pasitikite įmonių naudojančių biometrines technologijas tinkamu asmens duomenų saugojimu?

- ☐ Taip
☐ Ne
☐ Nežinau/ar neturiu nuomonės

15. Kiek Jums yra svarbu, kad būtų suteikta galimybė kontroliuoti savo biometrinių duomenų naudojimą (pvz., galimybė atšaukti savo suteiktą sutikimą)?

- ☐ Labai svarbu
☐ Gana svarbu
☐ Nėra itin svarbu
☐ Visiškai nesvarbu
☐ Nežinau/ar neturiu nuomonės

16. Kokia Jūsų pozicija, dėl biometrinių technologijų naudojimo viešoje erdvėje (pvz., viešojo transporto stotyse, oro uostuose, prekybos centruose)?

- ☐ Visiškai sutinku
☐ Šiek tiek sutinku
☐ Šiek tiek nesutinku
☐ Visiškai nesutinku

17. Ar manote, kad viešoje erdvėje reikia daugiau informacijos apie biometrinių technologijų naudojimą, jų poveikį asmens duomenų apsaugai ir kad švietimas šioje srityje turėtų būti didinamas?

- ☐ Taip
☐ Ne
☐ Nežinau/ar neturiu nuomonės

18. Ar būtumėte pasirengęs mokėti daugiau už produktą ar paslaugą, naudojančią saugesnes biometrines technologijas?

- ☐ Taip
☐ Ne
☐ Nežinau/ar neturiu nuomonės

19. Ar manote, kad vartotojų teisės yra pakankamai apsaugotos biometrinių technologijų naudojimo srityje?

- ☐ Taip, mano nuomone, teisės yra gerai apsaugotos
☐ Šiek tiek, galbūt galėtų būti geresnė apsauga
☐ Ne, mano nuomone, teisės nėra pakankamai apsaugotos

☐ Nežinau/ar neturiu nuomonės

20. Ar esate patenkintas dabartiniu biometrinių technologijų lygiu, siekiant apsaugant savo asmeninius duomenis?

- ☐ Labai nepatenkintas
- ☐ Šiek tiek nepatenkintas
- ☐ Nei patenkintas, nei nepatenkintas)
- ☐ Šiek tiek patenkintas
- ☐ Labai patenkintas

21. Ar jums kelia nerimą galimybė, kad jūsų biometriniai duomenys gali būti perduoti trečiosioms šalims?

- ☐ Taip
- ☐ Ne
- ☐ Nežinau/ar neturiu nuomonės

22. Ar esate susipažinęs/-usi su Lietuvos ar Europos Sąjungos teisės aktais, reglamentuojančiais biometrinių duomenų naudojimą?

- ☐ Taip, gerai susipažinęs/-usi
- ☐ Šiek tiek susipažinęs/-usi
- ☐ Ne, nesu susipažinęs/-usi

23. Ar kada nors patyrėte savo asmens duomenų vagystę arba buvote susipažinęs/-usi su atvejais, kai buvo pavogti kiti žmonių asmens duomenys?

- ☐ Taip, buvau patyręs/-usi savo asmens duomenų vagystę
- ☐ Buvau susipažinęs/-usi su kitų žmonių asmens duomenų vagystės atvejais
- ☐ Ne, niekada nesu patyręs/-usi ar susidūręs/-usi su tokiais atvejais
- ☐ Nežinau/ar neturiu nuomonės

24. Ar yra tekę susidurti su biometrinių technologijų klaidomis ar trūkumų atvejais atpažįstant asmens tapatybę?

- ☐ Taip, turėjau problemų, dėl biometrinių technologijų klaidų ar trūkumų
- ☐ Ne, nesu patyręs/-usi problemų su biometrinėmis technologijomis
- ☐ Nežinau/ar neturiu nuomonės

Ačiū, kad skyrėte savo laiką ir sudalyvavote apklausoje

Priedas 3. Patvirtinimas apie atlikto darbo savarankiškumą**PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ**

2023-04-26

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

Viešojo valdymo ir verslo fakulteto, kibernetinio saugumo valdymo*(fakulteto / instituto, programos pavadinimas)*Studentas (-ė) **Edgaras Sriubas***(vardas, pavardė)*patvirtinu, kad šis rašto darbas / bakalauro / **magistro baigiamasis darbas****„Biometrinių technologijų plėtros grėsmės asmens duomenų apsaugai“:**

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

Edgaras Sriubas*(parašas)**(vardas, pavardė)*